GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DOS DADOS

1471/14/PT
WP 223

Parecer 8/2014 sobre os recentes desenvolvimentos na Internet das Coisas

Adotado em 16 de setembro de 2014

O GRUPO DE TRABALHO PARA A PROTEÇÃO DAS PESSOAS NO QUE DIZ RESPEITO AO TRATAMENTO DE DADOS PESSOAIS

Instituído pela Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995,

Tendo em conta os artigos 29.º e 30.º da referida diretiva,

Tendo em conta o seu regulamento interno,

ADOTOU O PRESENTE PARECER:

SÍNTESE

A Internet das Coisas (IdC) encontra-se no limiar da integração na vida normal dos cidadãos europeus. A viabilidade de muitos projetos no domínio da IdC continua por confirmar, mas estão a ser disponibilizadas «coisas inteligentes» que monitorizam e comunicam com as nossas casas, carros, ambiente de trabalho e atividades físicas. Hoje em dia, os dispositivos conectados já satisfazem com êxito as necessidades dos cidadãos da UE nos mercados em grande escala do «eu quantificado» e da domótica. Assim, a IdC possui perspetivas de crescimento significativas para um grande número de empresas inovadoras e criativas da UE, grandes ou pequenas, que operam nestes mercados.

O Grupo de Trabalho do artigo 29.º (a seguir designado «Grupo de Trabalho») está empenhado na satisfação de tais expectativas, no interesse dos cidadãos e da indústria da UE. No entanto, estes benefícios esperados devem também respeitar os muitos desafios de privacidade e de segurança que podem estar associados à IdC. Surgem muitas questões em torno da vulnerabilidade destes dispositivos, muitas vezes instalados fora de uma estrutura informática tradicional e com uma segurança incorporada insuficiente. As perdas de dados e as infeções por vírus malévolos (*malware*), mas também o acesso não autorizado aos dados pessoais, a utilização intrusiva de dispositivos vestíveis ou a vigilância ilegal, são riscos que as partes interessadas na IdC devem abordar para atrair potenciais utilizadores finais dos seus produtos ou serviços.

Além da conformidade legal e técnica, o que está em causa são, de facto, as consequências que a IdC poderá ter para a sociedade em geral. As organizações que colocarem a privacidade e a proteção dos dados na vanguarda do desenvolvimento de produtos estarão bem posicionadas para garantir que os seus bens e serviços respeitam os princípios da privacidade desde a conceção e estão equipados com as predefinições respeitadoras da privacidade esperadas pelos cidadãos da UE.

Por enquanto, esta análise apenas foi referida em termos muito gerais por uma série de entidades reguladoras e partes interessadas na UE e não só. O Grupo de Trabalho decidiu levar esta questão mais além através da adoção do presente parecer. Deste modo, tenciona contribuir para a aplicação uniforme do quadro jurídico em matéria de proteção de dados à IdC, bem como para o desenvolvimento de um elevado nível de proteção no que diz respeito à proteção de dados pessoais na UE. A conformidade com este quadro é fundamental para dar resposta aos desafios jurídicos e técnicos, mas também, e uma vez que se baseia na qualificação da proteção de dados como um direito humano fundamental, aos desafios societais acima descritos.

Por conseguinte, o presente parecer identifica os principais riscos para a proteção de dados existentes no ecossistema da IdC, antes de fornecer orientações sobre o modo como o quadro jurídico da UE deve ser aplicado neste contexto. O Grupo de Trabalho apoia a incorporação das garantias mais elevadas possíveis para os utilizadores individuais no cerne dos projetos pelas partes interessadas. Concretamente, os utilizadores devem manter o controlo completo dos seus dados pessoais em todo o ciclo de vida do produto, e sempre que as organizações dependerem do consentimento como base para o tratamento dos dados, este deve ser plenamente informado, livre e específico. Para os ajudar a atingir este fim, o Grupo de Trabalho elaborou um amplo conjunto de recomendações práticas dirigidas às diferentes partes interessadas em causa (fabricantes de dispositivos, criadores de aplicações, plataformas sociais, destinatários ulteriores de dados, plataformas de dados e organismos de normalização) para as ajudar a aplicar a privacidade e a proteção de dados nos seus produtos e serviços.

Com efeito, capacitar as pessoas mantendo-as informadas, livres e seguras é essencial para apoiar a confiança e a inovação e, por conseguinte, para o sucesso nestes mercados. O Grupo de Trabalho está

convicto de que as partes interessadas que satisfaçam tais expectativas terão uma vantagem concorrencial excecionalmente forte em relação aos outros intervenientes cujos modelos de negócios se baseiam em manter os clientes na ignorância sobre o tratamento e a partilha dos seus dados e em prendê-los nos seus ecossistemas.

Tendo em conta os principais desafios da proteção de dados suscitados pela IdC, o Grupo de Trabalho continuará a acompanhar a sua evolução. Para tal, mantém-se aberto à cooperação com outras entidades reguladoras e legisladores nacionais ou internacionais sobre estas questões. Também se mantém aberto ao debate com representantes da sociedade civil e do setor relevante, em especial sempre que as partes interessadas operem na qualidade de responsável pelo tratamento de dados ou de subcontratante na UE.

INTRODUÇÃO

O conceito de Internet das Coisas (IdC) refere-se a uma infraestrutura em que milhares de milhões de sensores integrados em dispositivos comuns, do dia-a-dia («coisas», efetivamente, ou coisas ligadas a outros objetos ou indivíduos), são concebidos para registar, tratar, armazenar e transferir dados e, uma vez que estão associados a identificadores únicos, interagir com outros dispositivos ou sistemas que utilizam capacidades de ligação em rede. Uma vez que se baseia no princípio do tratamento extensivo de dados através destes sensores que são concebidos para comunicar discretamente e trocar dados de forma contínua, a IdC está estreitamente ligada às noções de computação «invasiva» e «omnipresente».

As partes interessadas na IdC pretendem oferecer novas aplicações e serviços através da recolha e da posterior combinação destes dados sobre os indivíduos, seja para «apenas» analisar os dados específicos do ambiente do utilizador, ou para observar e analisar especificamente os seus hábitos. Por outras palavras, a IdC implica geralmente o tratamento de dados que dizem respeito a pessoas singulares identificadas ou identificáveis qualificando-se, por conseguinte, como dados pessoais na aceção do artigo 2.º da Diretiva Proteção de Dados da UE.

O tratamento desses dados neste contexto baseia-se na intervenção coordenada de um número significativo de partes interessadas (isto é, fabricantes de dispositivos, que por vezes também atuam como plataformas de dados, agregadores de dados ou corretores, criadores de aplicações, plataformas sociais, emprestadores ou alugadores de dispositivos, etc.). Os respetivos papéis destas partes interessadas serão analisados mais adiante no presente parecer. Estas diferentes partes interessadas podem estar envolvidas por vários motivos, nomeadamente para fornecer funcionalidades adicionais ou interfaces de controlo de fácil utilização que permitem a gestão das configurações técnicas e de privacidade, ou porque o utilizador terá habitualmente acesso aos seus dados recolhidos através de uma interface web distinta. Além disso, assim que os dados são armazenados à distância, podem ser partilhados com outras partes, por vezes sem o conhecimento do seu titular[1]. Nestes casos, a transmissão ulterior dos seus dados é, por conseguinte, imposta ao utilizador, que não a pode impedir sem desativar a maior parte das funcionalidades do dispositivo. Na sequência desta cadeia de ações, a IdC pode colocar os fabricantes de dispositivos e os seus parceiros comerciais em condições de construir ou aceder a perfis de utilizador muito pormenorizados.

[1] http://www.ftc.gov/system/files/documents/public_events/195411/consumer-health-data-webcast-slides.pdf

Tendo em conta o que precede, o desenvolvimento da IdC levanta claramente desafios novos e significativos em matéria de proteção dos dados pessoais e de privacidade[2]. De facto, se não forem controlados, alguns desenvolvimentos da IdC podem até implicar uma forma de vigilância das pessoas suscetível de ser considerada ilegal nos termos da legislação da UE. A IdC suscita, igualmente, preocupações importantes em matéria de segurança, uma vez que as quebras de segurança podem implicar riscos de privacidade significativos para os indivíduos cujos dados são tratados nesses contextos.

O Grupo de Trabalho do artigo 29.º decidiu, por conseguinte, emitir o presente parecer a fim de contribuir para a identificação e a monitorização dos riscos resultantes dessas atividades, em que estão em causa os direitos fundamentais dos cidadãos da UE.

[2] O presente parecer deve ler-se também em ligação com os pareceres anteriores adotados pelo Grupo de Trabalho em 2014, nomeadamente os seus pareceres sobre a aplicação dos conceitos de necessidade e proporcionalidade e a proteção de dados no setor da aplicação coerciva da lei (WP 211) e sobre a vigilância (WP 215).

1. Âmbito do parecer: atenção especial a três desenvolvimentos na IdC

Nesta fase, é impossível prever com certeza o alcance da evolução da IdC, em parte porque permanece amplamente em aberto a questão do modo como se dá a transformação de todos os dados eventualmente recolhidos na IdC em algo útil e, por conseguinte, comercialmente viável. Também pouco claras são as possíveis convergências e sinergias da IdC com outros avanços tecnológicos, tais como a computação em nuvem e a analítica preditiva que, nesta fase, dizem respeito apenas a avanços de mercados emergentes.

O Grupo de Trabalho decidiu, por conseguinte, centrar-se, neste parecer, essencialmente em três desenvolvimentos específicos a nível da IdC (computação vestível, eu quantificado e domótica) que (1) estão em interface direta com o utilizador e (2) correspondem a dispositivos e serviços que estão atualmente em utilização e que, por conseguinte, se prestam a uma análise ao abrigo da legislação em matéria de proteção de dados. Este parecer, portanto, não trata especificamente das aplicações B2B (empresa a empresa) e de questões mais globais como as «cidades inteligentes» e os «transportes inteligentes», nem dos avanços a nível das tecnologias M2M («máquina a máquina»). No entanto, os princípios e as recomendações formulados no presente parecer podem aplicar-se fora do seu âmbito estrito e abranger esses outros desenvolvimentos a nível da IdC.

1.1 **Computação vestível**

A computação vestível refere-se a objetos do dia-a-dia e a vestuário, como relógios e óculos, que incluem sensores destinados a ampliar as suas funcionalidades. É provável que as coisas vestíveis sejam adotadas rapidamente, uma vez que alargam a utilidade dos objetos do dia-a-dia que são familiares aos indivíduos, inclusivamente por não se distinguirem com facilidade de outros objetos não conectados. Podem incorporar câmaras, microfones e sensores que podem gravar e transferir dados para o fabricante de dispositivos. Além disso, a disponibilidade de uma API (interface de programação de aplicações) para dispositivos vestíveis (por exemplo, o Android Wear[3]) fomenta a criação de aplicações por terceiros que podem, assim, obter acesso aos dados recolhidos por essas coisas.

1.2 **Eu quantificado**

As coisas do «eu quantificado» são concebidas para serem transportadas regularmente por pessoas que desejam registar informações sobre os seus próprios hábitos e estilos de vida. Por exemplo, um indivíduo pode querer usar todas as noites um monitorizador de sono para obter um panorama amplo dos seus padrões de sono. Outros dispositivos centram-se no registo dos movimentos, como os contadores de atividade, que medem e comunicam continuamente indicadores quantitativos relacionados com as atividades físicas do indivíduo, como as calorias queimadas ou as distâncias percorridas a pé, entre outras coisas.

Outros objetos medem o peso, o pulso e outros indicadores de saúde. Através da observação das tendências e das alterações no comportamento ao longo do tempo, os dados recolhidos podem ser analisados para extrair informações qualitativas relacionadas com a saúde, incluindo avaliações sobre a qualidade e os efeitos da atividade física, com base em certos limiares previamente fixados, bem como, em certa medida, a presença provável de sintomas de doença.

Os sensores do eu quantificado têm, frequentemente, de ser usados em condições específicas para extraírem informações relevantes. Por exemplo, um acelerómetro colocado no cinto de uma pessoa, com os algoritmos adequados, pode medir os movimentos do abdómen *(dados brutos)*, extrair

[3] http://developer.android.com/wear/index.html

informação sobre o ritmo da sua respiração *(dados agregados e informação extraída)* e apresentar o nível de stresse do titular dos dados *(dados apresentáveis)*. Em alguns dispositivos, só é comunicada ao utilizador esta última informação, mas o fabricante do dispositivo ou o prestador de serviços pode ter acesso a muito mais dados que podem ser analisados posteriormente.

O eu quantificado constitui um desafio no que diz respeito aos tipos de dados recolhidos relacionados com a saúde e, por conseguinte, potencialmente sensíveis, bem como à ampla recolha desses dados. Na verdade, por se centrar na motivação dos utilizadores para se manterem saudáveis, este movimento tem muitas ligações com o ecossistema da saúde em linha. Ainda assim, estudos recentes contestaram a exatidão real das medições e das inferências feitas a partir destas[4].

1.3 **Automação residencial («domótica»)**

Hoje em dia, os dispositivos IdC também podem ser colocados em escritórios ou residências, como lâmpadas, termóstatos, detetores de fumo, estações meteorológicas, máquinas de lavar ou fornos «conectados» que podem ser controlados à distância pela Internet. Por exemplo, as coisas que contêm sensores de movimento podem detetar e registar quando um utilizador está em casa e quais são os seus padrões de movimento e talvez desencadear ações específicas previamente identificadas (por exemplo, ligar uma luz ou alterar a temperatura da divisão). A maioria dos dispositivos de automação residencial está conectada continuamente e pode transmitir dados ao fabricante.

Obviamente, a domótica suscita desafios específicos em matéria de proteção de dados e de privacidade, uma vez que uma análise dos padrões de utilização neste contexto é suscetível de revelar pormenores acerca do estilo de vida, dos hábitos ou das opções dos habitantes, ou simplesmente a sua presença em casa.

As três categorias de dispositivos supramencionadas são exemplares da maioria das principais questões associadas à privacidade relacionadas com a IdC no seu estado atual. Convém salientar, no entanto, que estas categorias não são exclusivas: por exemplo, um dispositivo «vestível», como um relógio inteligente, pode ser utilizado para monitorização da frequência cardíaca, ou seja, para uma avaliação do eu quantificado.

2. Desafios em matéria de privacidade e proteção de dados relacionados com a Internet das Coisas

O Grupo de Trabalho decidiu emitir este parecer específico por considerar que a IdC suscita uma série de questões relevantes em matéria de privacidade e proteção de dados, algumas novas e outras mais tradicionais, mas amplificadas no que se refere ao aumento exponencial do tratamento de dados envolvido na sequência da sua evolução. A importância da aplicação do quadro jurídico da UE em matéria de proteção de dados e das recomendações práticas correspondentes a seguir formuladas deve ser considerada à luz dessas questões.

2.1 **Falta de controlo e assimetria da informação**

Como resultado da necessidade de prestar serviços invasivos de uma forma discreta, os utilizadores podem, na prática, encontrar-se sob monitorização de terceiros. Isto pode resultar em situações em que o utilizador pode perder o controlo da divulgação dos seus dados, dependendo da transparência com que é feita a recolha e o tratamento desses dados.

[4] http://bits.blogs.nytimes.com/2014/04/27/for-fitness-bands-slick-marketing-but-suspect-results

De um modo mais geral, a interação entre objetos, entre objetos e os dispositivos dos indivíduos, entre indivíduos e outros objetos e entre objetos e sistemas de retaguarda resultará na geração de fluxos de dados que dificilmente podem ser geridos com as ferramentas clássicas utilizadas para assegurar uma proteção adequada dos interesses e dos direitos dos titulares dos dados. Por exemplo, ao contrário de outros tipos de conteúdos, os dados extraídos pela IdC podem não ser devidamente revistos pela pessoa em causa antes da sua publicação, o que gera, inegavelmente, um risco de falta de controlo e de autoexposição excessiva para o utilizador. Além disso, a comunicação entre objetos pode ser desencadeada automaticamente, bem como por predefinição, sem o conhecimento do indivíduo. Na ausência da possibilidade de controlar eficazmente o modo como os objetos interagem ou de poder definir fronteiras virtuais através da definição de zonas ativas ou não ativas para coisas específicas, vai tornar-se extremamente difícil controlar os fluxos de dados gerados. Vai ser ainda mais difícil controlar a sua utilização subsequente e impedir, desse modo, o potencial desvirtuamento da função. Este problema de falta de controlo, que também diz respeito a outros avanços técnicos, como a computação em nuvem ou os grandes volumes de dados, é ainda mais desafiante quando se pensa que estas diferentes tecnologias emergentes podem ser utilizadas em combinação.

2.2 **Qualidade do consentimento do utilizador**

Em muitos casos, o utilizador pode não ter conhecimento do tratamento de dados efetuado por objetos específicos. Essa falta de informação constitui um obstáculo significativo à manifestação de consentimento válido ao abrigo da legislação da UE, uma vez que o titular dos dados tem de estar informado. Em tais circunstâncias, o consentimento não pode ser invocado como base legal para o tratamento de dados correspondente ao abrigo da legislação da UE.

Os dispositivos vestíveis, como os relógios inteligentes, também não são detetáveis[5]: a maior parte dos observadores não consegue distinguir um relógio normal de um relógio conectado, quando este último pode incorporar câmaras, microfones e sensores de movimento capazes de registar e transferir dados sem o conhecimento dos indivíduos e sem o seu consentimento nesse tratamento. Isto suscita a questão da identificação do tratamento de dados através de computação vestível, que pode ser resolvida prevendo uma sinalização adequada que seja efetivamente visível para os titulares dos dados.

Além disso, pelo menos em alguns casos, a possibilidade de renunciar a determinados serviços ou funcionalidades de um dispositivo IdC é mais um conceito teórico do que uma alternativa real. Estas situações conduzem à questão de saber se o consentimento do utilizador para o tratamento de dados subjacente pode ser considerado como livre e, por conseguinte, válido ao abrigo da legislação da UE.

Além disso, os mecanismos clássicos utilizados para obter o consentimento dos indivíduos podem ser difíceis de aplicar na IdC, resultando num consentimento de «baixa qualidade» baseado na falta de informação ou na impossibilidade factual de conceder um consentimento ajustado em conformidade com as preferências expressas pelos indivíduos. Na prática, hoje em dia afigura-se que os dispositivos sensores não são geralmente concebidos para prestar informações sobre si próprios nem para proporcionar um mecanismo válido para obter o consentimento do indivíduo. Ainda assim, as partes interessadas na IdC devem ponderar novas formas de obter o consentimento válido do utilizador, nomeadamente pela aplicação de mecanismos de consentimento através dos próprios dispositivos. São

[5] Tal como descrito no Parecer 02/2013 sobre as aplicações em dispositivos inteligentes, a computação vestível também realça os desafios decorrentes da recolha de dados contínua por terceiros nas proximidades e por períodos extensos de tempo.

apresentados mais adiante neste documento exemplos específicos, como *proxies* para privacidade e «sticky policies» (políticas associadas aos dados).

2.3 **Inferências derivadas de dados e redefinição da finalidade do tratamento inicial**

O aumento da quantidade de dados gerados pela combinação da IdC com técnicas modernas relacionadas com a análise e o cruzamento de dados poderá tornar esses dados suscetíveis a utilizações secundárias, relacionadas ou não com a finalidade do tratamento inicial. Terceiros que solicitem o acesso aos dados recolhidos por outras partes podem, por conseguinte, querer utilizar esses dados para fins totalmente diferentes.

Dados aparentemente insignificantes recolhidos inicialmente através de um dispositivo (por exemplo, o acelerómetro e o giroscópio de um *smartphone*) podem vir a ser utilizados para extrair outras informações com um significado totalmente diferente (por exemplo, os hábitos de condução do indivíduo). Esta possibilidade de fazer extrações a partir dessas informações «em bruto» deve ser combinada com os riscos clássicos analisados no que diz respeito à fusão de sensores, um fenómeno bem conhecido em informática[6].

O eu quantificado ilustra igualmente a quantidade de informação que pode ser inferida a partir de sensores de movimento através da agregação e da análise avançada. Estes dispositivos utilizam, muitas vezes, sensores elementares para captar dados brutos (por exemplo, movimentos do titular dos dados) e baseiam-se em algoritmos sofisticados para extrair informação sensível (por exemplo, o número de passos) e deduzir informações potencialmente sensíveis que serão apresentadas aos utilizadores finais (por exemplo, a sua condição física).

Esta tendência suscita problemas específicos. Com efeito, apesar de não se opor à partilha da informação inicial para um fim específico, o utilizador pode não querer partilhar essas informações secundárias que podem ser utilizadas para fins totalmente diferentes. Por conseguinte, é importante que, em cada nível (dados brutos, extraídos ou apresentados), as partes interessadas na IdC se certifiquem de que os dados são utilizados para fins compatíveis com a finalidade inicial do tratamento e que essa finalidade seja do conhecimento do utilizador.

2.4 **Provocação invasiva de padrões de comportamento e definição de perfis**

Embora objetos diferentes recolham separadamente elementos de informação isolados, uma quantidade suficiente de dados recolhidos e posteriormente analisados pode revelar aspetos específicos dos hábitos, comportamentos e preferências de um indivíduo. Como concluímos anteriormente, a geração de conhecimento a partir de dados triviais ou até anónimos será facilitada pela proliferação de sensores e promoverá capacidades importantes de definição de perfis.

Além disso, a analítica baseada nas informações capturadas num ambiente IdC pode permitir a deteção ainda mais pormenorizada e completa da vida de um indivíduo e dos seus padrões de comportamento.

Na verdade, é provável que esta tendência venha a influenciar a forma como o indivíduo efetivamente se comporta, do mesmo modo que ficou demonstrado que a utilização intensiva de câmaras de vigilância influenciou o comportamento dos cidadãos em espaços públicos. Com a IdC, essa potencial vigilância pode agora alcançar a esfera mais privada da vida dos indivíduos, incluindo as suas casas.

[6] A fusão de sensores consiste em combinar dados de sensores ou dados provenientes de fontes diferentes a fim de obter informação melhor e mais precisa do que a que seria possível obter no caso de estas fontes estarem a funcionar isoladamente.

Deste modo, o indivíduo será pressionado a evitar comportamentos não habituais, a fim de prevenir a deteção de tudo o que possa ser entendido como uma anomalia. Essa tendência seria muito invasiva da vida privada e da intimidade dos indivíduos e deverá ser acompanhada de muito perto.

2.5 **Limitações à possibilidade de manter o anonimato ao utilizar serviços**

O pleno desenvolvimento das capacidades da IdC pode colocar pressão sobre as atuais possibilidades de utilização anónima de serviços e, em geral, limitar a possibilidade de passar despercebido.

Por exemplo, as coisas vestíveis mantidas na proximidade imediata dos titulares dos dados resultam na disponibilidade de uma série de outros identificadores, tais como os endereços MAC de outros dispositivos que podem ser úteis para gerar uma impressão digital que permita localizar o titular dos dados. A recolha de múltiplos endereços MAC de múltiplos dispositivos sensores ajudará a criar impressões digitais únicas e identificadores mais estáveis que as partes interessadas na IdC poderão atribuir a indivíduos específicos. Essas impressões digitais e identificadores poderiam ser utilizados para vários fins, incluindo a analítica da localização[7] ou a análise dos padrões de movimento de multidões e indivíduos.

Esta tendência deve ser combinada com o facto de esses dados poderem depois ser combinados com outros dados provenientes de outros sistemas (por exemplo, câmaras de vigilância ou registos da Internet).

Nestas circunstâncias, alguns dados dos sensores são particularmente vulneráveis a ataques de reidentificação.

Tendo em conta o que precede, é evidente que se tornará cada vez mais difícil manter o anonimato e preservar a privacidade na IdC. A esse respeito, o desenvolvimento da IdC suscita preocupações significativas em matéria de privacidade e proteção de dados.

2.6 **Riscos de segurança: segurança *versus* eficiência**

A IdC levanta vários problemas de segurança, inclusivamente porque os condicionalismos em matéria de segurança e de recursos obrigam os fabricantes de dispositivos a equilibrar a eficiência da bateria e a segurança do dispositivo. Mais concretamente, ainda não é claro o modo como os fabricantes de dispositivos irão equilibrar a aplicação de medidas de confidencialidade, integridade e disponibilidade a todos os níveis da sequência de tratamento de dados com a necessidade de otimizar a utilização de recursos computacionais (e de energia) pelos objetos e sensores.

Por conseguinte, existe um risco de que a IdC possa transformar um objeto do dia-a-dia num potencial alvo de ataque à privacidade e à segurança de informação ao fazer uma distribuição muito mais alargada desses alvos do que a atual versão da Internet. Os dispositivos conectados menos seguros representam novas formas de ataque potencialmente eficazes, nomeadamente facilitando as práticas de vigilância e as violações de dados que resultam no roubo ou comprometimento de dados pessoais que podem ter efeitos generalizados sobre os direitos dos consumidores e sobre a perceção da segurança da IdC por parte dos indivíduos.

É, além disso, esperado que os dispositivos e plataformas IdC troquem dados e os armazenem em infraestruturas dos prestadores de serviços. Por conseguinte, a segurança da IdC não deve ser planeada

[7] A analítica da localização refere-se à análise de quantas pessoas se encontram em determinado local num determinado momento e por quanto tempo permanecem nesse local.

tendo em conta apenas a segurança dos dispositivos, mas também as ligações de comunicação, a infraestrutura de armazenamento e outros contributos deste ecossistema.

Do mesmo modo, a presença de diferentes níveis de tratamento cuja conceção técnica e aplicação são fornecidas por diferentes partes interessadas, não assegura a coordenação adequada entre todos eles e pode resultar na presença de pontos fracos capazes de serem utilizados para explorar vulnerabilidades.

Por exemplo, a maioria dos sensores atualmente existentes no mercado não é capaz de estabelecer uma ligação encriptada nas suas comunicações, uma vez que os requisitos de computação terão repercussões num dispositivo limitado por baterias de baixo consumo de energia. No que diz respeito à segurança extremo a extremo, o resultado da integração dos componentes físicos e lógicos fornecidos por um conjunto de diferentes partes interessadas apenas garante o nível de segurança assegurado pelo componente mais fraco.

3. Aplicabilidade da legislação da UE ao tratamento de dados pessoais na IdC

3.1 **Lei aplicável**

O quadro jurídico relevante para avaliar as questões de privacidade e proteção de dados suscitadas pela IdC na UE é composto pela Diretiva 95/46/CE, bem como pelas disposições específicas da Diretiva 2002/58/CE, conforme alterada pela Diretiva 2009/136/CE.

Este quadro aplica-se sempre que estejam preenchidas as condições para a sua aplicabilidade previstas no artigo 4.º da Diretiva 95/46/CE. O Grupo de Trabalho forneceu orientações extensas sobre a interpretação do disposto no artigo 4.º, nomeadamente no seu Parecer 8/2010[8] sobre a lei aplicável.

Em particular, nos termos do artigo 4.º, n.º1, alínea a), da diretiva, o direito nacional de um Estado-Membro é aplicável a todo o tratamento de dados pessoais efetuado «no contexto das atividades de um estabelecimento» do responsável pelo tratamento situado no território desse Estado-Membro. Esta noção de estabelecimento no contexto da economia baseada na Internet foi recentemente interpretada de forma muito abrangente pelo Tribunal de Justiça Europeu[9].

O direito nacional de um Estado-Membro é igualmente aplicável nos casos em que o responsável pelo tratamento não estiver estabelecido no território da Comunidade e recorrer a meios situados no território desse Estado-Membro (artigo 4.º, n.º 1, alínea c)). Por conseguinte, mesmo quando uma parte interessada na IdC, que se qualifique como um responsável pelo tratamento ao abrigo da Diretiva 95/46/CE, não está estabelecida na UE na aceção do artigo 4.º, n.º 1, alínea a) (quer esteja envolvida no desenvolvimento, na distribuição ou na operação dos dispositivos IdC), essa parte interessada ainda estará provavelmente sujeita à legislação da UE, na medida em que efetua o tratamento dos dados recolhidos através dos «meios» dos utilizadores localizados na UE.

Com efeito, todos os objetos que são utilizados para recolher e posteriormente tratar dados de indivíduos no contexto da prestação de serviços em IdC são considerados como meios na aceção da diretiva. Esta qualificação aplica-se, obviamente, aos próprios dispositivos (contadores de passos, monitorizadores de sono, dispositivos residenciais «conectados» como termóstatos, detetores de fumo, óculos ou relógios conectados, etc.). Aplica-se igualmente aos dispositivos terminais dos utilizadores (por exemplo, *smartphones* ou *tablets*) nos quais tenha sido previamente instalado *software* ou

[8] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_pt.pdf
[9] Acórdão do Tribunal de Justiça (Grande Secção), 13 de maio de 2014, processo C-131/12 (números 45 a 60).

aplicações para monitorizar o ambiente do utilizador através de sensores integrados ou interfaces de rede e para, em seguida, enviar os dados recolhidos por estes dispositivos para os vários responsáveis pelo tratamento envolvidos.

A identificação do papel das diferentes partes interessadas envolvidas na IdC será essencial para qualificar o seu estatuto jurídico como responsáveis pelo tratamento de dados e, desse modo, identificar a legislação nacional aplicável ao tratamento que aplicam, bem como as respetivas responsabilidades. A identificação do papel das partes envolvidas na IdC será analisada a seguir, na secção 3.3.

3.2 **A noção de dados pessoais**

A legislação da UE é aplicável ao tratamento de dados pessoais na aceção do artigo 2.º da Diretiva 95/46/CE. O Grupo de Trabalho forneceu orientações extensas sobre a interpretação desta noção, nomeadamente no seu Parecer 04/2007 sobre o conceito de dados pessoais[10].

No contexto da IdC, acontece frequentemente uma pessoa poder ser identificada com base em dados provenientes de «coisas». Com efeito, esses dados podem permitir distinguir o padrão de vida de um determinado indivíduo ou família – por exemplo, os dados gerados através do controlo centralizado da iluminação, do aquecimento, da ventilação e do ar condicionado.

Além disso, mesmo os dados relativos a indivíduos que se destinam a ser tratados apenas após a aplicação de pseudonimização, ou até de técnicas de anonimização, podem ter de ser considerados como dados pessoais. Na verdade, a grande quantidade de dados tratados automaticamente no contexto da IdC implica riscos de reidentificação. A este respeito, o Grupo de Trabalho remete para os desenvolvimentos relevantes descritos no seu recente parecer sobre técnicas de anonimização, que ajuda a identificar estes riscos e formula recomendações sobre a aplicação destas técnicas[11].

3.3 **Partes interessadas na IdC como responsáveis pelo tratamento sediados na UE**

O conceito de responsável pelo tratamento e a sua interação com o conceito de subcontratante são centrais na aplicação da Diretiva 95/46/CE, uma vez que condicionam as responsabilidades das várias organizações envolvidas na execução de um tratamento de dados no que diz respeito às regras de proteção de dados da UE. As partes interessadas podem consultar o Parecer 1/2010 do Grupo de Trabalho sobre os conceitos de «responsável pelo tratamento» e «subcontratante»[12], que fornece orientações sobre a aplicação deste conceito a sistemas complexos com múltiplos intervenientes, onde muitos cenários envolvem responsáveis pelo tratamento e subcontratantes, isolada ou conjuntamente, com diferentes graus de autonomia e responsabilidade.

Com efeito, a aplicação da IdC implica, casualmente, a intervenção combinada de várias partes interessadas, tais como fabricantes de dispositivos, plataformas sociais, aplicações de terceiros, emprestadores ou alugadores de dispositivos, corretores de dados[13] ou plataformas de dados.

---

[10] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_pt.pdf

[11] Parecer 05/2014 sobre técnicas de anonimização, adotado em 10 de abril de 2014 (WP 216), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_pt.pdf

[12] Parecer 01/2010 sobre os conceitos de «responsável pelo tratamento» e «subcontratante», adotado em 16 de fevereiro de 2010 (WP 169) http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_pt.pdf

[13] Os corretores de dados compram dados das empresas para criar listas de indivíduos pertencentes a uma mesma categoria ou grupo. Estas categorias e grupos são definidos pelos corretores de dados, mas podem refletir atributos demográficos, rendimentos ou interesse manifesto por um tema ou produto específico.

A rede complexa de partes interessadas envolvidas requer/implica a necessidade de uma repartição precisa das responsabilidades jurídicas entre elas no que diz respeito ao tratamento de dados pessoais do indivíduo, com base nas especificidades das respetivas intervenções.

3.3.1 Fabricantes de dispositivos

Os fabricantes de dispositivos da IdC fazem mais do que apenas vender artigos físicos aos seus clientes ou produtos de marca branca a outras organizações. Podem também ter desenvolvido ou modificado o sistema operativo da «coisa» ou instalado *software* que determine a sua funcionalidade global, incluindo dados e a frequência da recolha de dados, quando e a quem os dados são transmitidos e para que fins (por exemplo, as empresas poderiam fixar o preço do seguro dos seus trabalhadores com base em dados comunicados pelos dispositivos de monitorização que os obrigam a utilizar[14]). A maior parte deles recolhe e trata, efetivamente, os dados pessoais que são gerados pelo dispositivo para fins e meios que determinaram inteiramente. Qualificam-se, assim como responsáveis pelo tratamento ao abrigo da legislação da UE.

3.3.2 Plataformas sociais

As pessoas são ainda mais suscetíveis de utilizar coisas conectadas quando podem partilhar esses dados publicamente ou com outros utilizadores. Em concreto, os utilizadores de dispositivos de eu quantificado tendem a partilhar dados com outras pessoas em redes sociais para promover uma forma de competição positiva dentro do grupo.

Essa partilha de dados recolhidos e agregados por «coisas» em redes sociais é frequentemente feita de forma automática a partir do momento em que o utilizador configura a aplicação nesse sentido. A capacidade de partilha está geralmente incluída nas configurações padrão predefinidas das aplicações fornecidas pelo fabricante.

A agregação destes dados em plataformas sociais significa, por conseguinte, que lhes passam a ser aplicáveis responsabilidades específicas em matéria de proteção de dados. Uma vez que estes dados são introduzidos pelo utilizador, quando são tratados por redes sociais para fins distintos que elas próprias determinam, as redes sociais passam a qualificar-se como responsáveis pelo tratamento por direito próprio, na aceção da legislação da UE. Por exemplo, uma rede social pode utilizar informações recolhidas por um pedómetro para inferir que um determinado utilizador é um corredor regular e apresenta-lhe anúncios de ténis de corrida. As consequências desta qualificação foram descritas em pormenor no anterior parecer do Grupo de Trabalho do artigo 29.º sobre as redes sociais[15].

3.3.3 Criadores de aplicações de terceiros

Muitos sensores expõem API a fim de facilitar a criação de aplicações. Para utilizar estas aplicações, as pessoas têm de instalar aplicações de terceiros que lhes permitem aceder aos seus dados armazenados pelo fabricante de dispositivos. A instalação destas aplicações implica, frequentemente, conceder ao criador da aplicação acesso aos dados através da API.

Algumas aplicações podem compensar os utilizadores de coisas específicas, por exemplo uma aplicação desenvolvida por uma companhia de seguros de saúde pode recompensar os utilizadores de

[14] Com dispositivos de monitorização, os empregadores podem acompanhar o estado de saúde dos trabalhadores: http://www.advisory.com/Daily-Briefing/2013/01/04/With-tracking-devices-employers-may-track-workers-health

[15] Parecer 5/2009 sobre as redes sociais em linha, adotado em 12 de junho de 2009 (WP 163) - http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_pt.pdf

«coisas» de eu quantificado ou uma companhia de seguros de habitação pode desenvolver uma aplicação específica para garantir que os alarmes de incêndio conectados dos seus clientes estão corretamente configurados. A menos que estes dados sejam adequadamente anonimizados, esse acesso constitui um tratamento na aceção do artigo 2.º da Diretiva 95/46/CE, pelo que o criador da aplicação que organizou este acesso aos dados deve ser considerado como responsável pelo tratamento ao abrigo da legislação da UE.

Estas aplicações são tradicionalmente instaladas com base numa opção explícita. Com efeito, uma vez que tal acesso está sujeito ao consentimento prévio obrigatório do utilizador, este consentimento deve ser dado de forma clara, específica e informada. A prática revela, no entanto, que frequentemente os pedidos de autorização feitos por criadores de aplicações de terceiros não apresentam informações suficientes para que o consentimento do utilizador possa ser considerado específico e suficientemente informado e, por conseguinte, válido ao abrigo da legislação da UE (ver *infra*).

3.3.4 Outros terceiros

Outros terceiros, além dos fabricantes de dispositivos e dos criadores de aplicações de terceiros, podem utilizar dispositivos IdC para recolher e tratar informações sobre indivíduos. Por exemplo, as companhias de seguros de saúde podem querer oferecer pedómetros aos clientes para controlar a frequência com que fazem exercício[16] e adaptar os prémios do seguro de acordo com esses valores.

Ao contrário dos fabricantes de dispositivos, esses terceiros não têm qualquer controlo sobre o tipo de dados recolhidos pela coisa. Ainda assim, são considerados como responsáveis pelo tratamento no que diz respeito a estes tratamentos, na medida em que recolhem e armazenam os dados gerados por esses dispositivos IdC para fins específicos por eles determinados.

Exemplo: uma companhia de seguros lança um novo desafio e oferece um pedómetro aos subscritores que pretendam candidatar-se a tarifas mais baixas. Os subscritores que aceitam a oferta recebem um pedómetro configurado e registado pela companhia. Apesar de os subscritores poderem aceder aos dados registados pelo seu pedómetro, os dispositivos são propriedade da «FeelGood», que também tem acesso aos dados dos seus subscritores. Neste contexto, os subscritores devem ser considerados como titulares de dados e ter acesso à sua conta na aplicação de contagem de passos, enquanto a companhia de seguros se qualifica como responsável pelo tratamento.

3.3.5 Plataformas de dados IdC

Devido à ausência de normalização e interoperabilidade, a Internet das Coisas é, por vezes, vista como uma «Intranet das Coisas» em que cada fabricante definiu o seu próprio conjunto de interfaces e formato de dados. Os dados são, então, alojados em ambientes fortificados, que impedem, de modo eficaz, que os utilizadores transfiram (ou combinem) os seus dados de um dispositivo para outro.

No entanto, os *smartphones* e os *tablets* tornaram-se os portais de acesso naturais dos dados recolhidos através de muitos dispositivos IdC à Internet. Consequentemente, os fabricantes foram desenvolvendo progressivamente plataformas que visam alojar os dados recolhidos através destes dispositivos diferentes, a fim de centralizar e simplificar a sua gestão.

[16] Com dispositivos de monitorização, os empregadores podem acompanhar o estado de saúde dos trabalhadores: http://www.advisory.com/Daily-Briefing/2013/01/04/With-tracking-devices-employers-may-track-workers-health

Estas plataformas podem também ser consideradas como responsáveis pelo tratamento ao abrigo da legislação da UE em matéria de proteção de dados, quando o desenvolvimento destes serviços implica efetivamente a recolha dos dados pessoais dos utilizadores para os seus próprios fins.

3.4 **Indivíduos como titulares dos dados: assinantes, utilizadores e não utilizadores**

Os assinantes e, de uma forma mais geral, os utilizadores da IdC são considerados como titulares de dados ao abrigo da legislação da UE. Se os dados que recolhem e armazenam forem utilizados exclusivamente para utilização pessoal ou doméstica, são abrangidos pela chamada «isenção para fins domésticos» prevista na Diretiva 95/46/CE[17]. No entanto, na prática, o modelo de negócios da IdC implica que os dados do utilizador sejam transferidos sistematicamente para os fabricantes de dispositivos, para os criadores de aplicações e para outros terceiros que se qualificam como responsáveis pelo tratamento. A «isenção para fins domésticos» terá, por conseguinte, uma aplicação limitada no contexto da IdC.

O tratamento de dados na IdC pode igualmente dizer respeito a indivíduos que não são assinantes nem utilizadores efetivos da IdC. Por exemplo, os dispositivos vestíveis, como os óculos inteligentes, podem recolher dados sobre outras pessoas que não o proprietário do dispositivo. É importante salientar que este fator não implica que a legislação da UE não seja aplicável a estas situações. A aplicação das regras de proteção de dados da UE não é condicionada pela propriedade de um dispositivo ou terminal, mas pelo tratamento dos dados pessoais propriamente ditos, independentemente da pessoa a quem os dados dizem respeito.

4. Obrigações das partes interessadas na IdC

As partes interessadas na IdC que se qualificam como responsáveis pelo tratamento (quer isoladas, quer juntamente com outras) ao abrigo da legislação da UE devem cumprir as diferentes obrigações a que estão sujeitas, em aplicação da Diretiva 95/46/CE, bem como das disposições relevantes da Diretiva 2002/58/CE, se for caso disso. O presente parecer aborda apenas a aplicação das disposições que merecem uma atenção específica neste contexto, contudo esta concentração limitada não implica que outras disposições não sejam aplicadas.

4.1 **Aplicação do artigo 5.º, n.º 3, da Diretiva Privacidade e Comunicações Eletrónicas**

O artigo 5.º, n.º 3, da Diretiva 2002/58/CE é aplicável a situações em que uma parte interessada na IdC armazena informações ou obtém acesso a informações já armazenadas num dispositivo IdC, na medida em que os dispositivos IdC se qualifiquem como «equipamentos terminais» na aceção desta disposição[18]. Esta disposição exige que o assinante ou utilizador em causa consinta nesse armazenamento ou acesso para que as referidas ações sejam legítimas, a menos que sejam «estritamente necessários para fornecer um serviço [...] explicitamente solicitado pelo assinante ou pelo utilizador» [19]. Este requisito é particularmente importante, uma vez que as partes interessadas além do utilizador ou do assinante podem ter acesso a informações sensíveis do ponto de vista da privacidade que se encontrem armazenadas nesse equipamento terminal[20].

---

[17] Ver Parecer 5/2009 sobre as redes sociais em linha, adotado em 12 de junho de 2009 (WP 163).

[18] A noção de «equipamento terminal» referida no artigo 5.º, n.º 3, deve ser entendida do mesmo modo que a noção de «meios» a que se refere o artigo 4.º, n.º 1, alínea c) da Diretiva 95/46/CE.

[19] Parecer 02/2013 sobre as aplicações em dispositivos inteligentes (WP 202), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_pt.pdf

[20] Ver o considerando 25 da Diretiva 2002/58/CE.

O requisito de consentimento previsto no artigo 5.º, n.º 3, diz respeito sobretudo ao fabricante de dispositivos, mas também a todas as partes interessadas que pretendam aceder aos dados brutos agregados armazenados nesta infraestrutura. Aplica-se igualmente a qualquer responsável pelo tratamento que pretenda armazenar dados adicionais no dispositivo de um utilizador.

Nestas circunstâncias, as partes interessadas na IdC devem assegurar que o titular dos dados consentiu efetivamente em tal armazenamento e/ou acesso, após ter obtido informações claras e abrangentes do responsável pelo tratamento, nomeadamente a finalidade do tratamento.

Por conseguinte, o consentimento do utilizador deve ser obtido antes do acesso a informações gravadas no dispositivo que possam ser utilizadas para gerar uma impressão digital de qualquer dispositivo (incluindo dispositivos vestíveis). O Grupo de Trabalho já emitiu orientações sobre a noção de consentimento para a colocação de *cookies* ou de tecnologias de monitorização semelhantes no seu Documento de Trabalho 02/2013 (WP 208) e irá fornecer mais orientações sobre esta questão no seu futuro parecer sobre impressões digitais.

Exemplo: um pedómetro regista o número de passos dados pelo seu utilizador e armazena essa informação na sua memória interna. O utilizador instalou uma aplicação no computador para descarregar diretamente o número de passos do seu dispositivo. Se o fabricante de dispositivos pretender transferir os dados do pedómetro para os seus servidores, terá de obter o consentimento do utilizador, nos termos do artigo 5.º, n.º 3, da Diretiva 2002/58/CE.

Assim que o fabricante do dispositivo tiver transferido os dados para os seus servidores, apenas guarda dados agregados sobre o número de passos por minuto. Uma aplicação que solicite acesso a esses dados, na medida em que estejam armazenados no servidor do fabricante de dispositivos, não está sujeita ao disposto no artigo 5.º, n.º 3, da Diretiva Privacidade e Comunicações Eletrónicas, mas ao disposto na Diretiva 95/46/CE, no que diz respeito à legitimidade deste tratamento ulterior.

Além disso, o proprietário de um dispositivo IdC e a pessoa cujos dados serão monitorizados (o titular dos dados) podem ser pessoas diferentes. Esta situação pode conduzir a uma aplicação repartida do artigo 5.º, n.º 3, da Diretiva 2002/58/CE e da Diretiva 95/46/CE.

Exemplo: um serviço de aluguer de automóveis instala um dispositivo inteligente de localização de veículos nos seus automóveis para aluguer. Embora o serviço de aluguer de automóveis seja considerado o proprietário/assinante do dispositivo/serviço de localização, o indivíduo que aluga o automóvel é considerado como o utilizador do dispositivo. O artigo 5.º, n.º 3, exige, portanto, que o fabricante do dispositivo obtenha (pelo menos) o consentimento do utilizador do dispositivo, neste caso do indivíduo que aluga o automóvel. Além disso, a legitimidade do tratamento de dados pessoais relativos aos indivíduos que alugam os automóveis estará ainda sujeita aos requisitos do artigo 7.º da Diretiva 95/46/CE.

4.2 **Base jurídica para o tratamento (artigo 7.º da Diretiva 95/46/CE)**

As partes interessadas na IdC que se qualificam como responsáveis pelo tratamento (ver ponto 4.3 acima) têm de respeitar um dos requisitos enumerados no artigo 7.º desta diretiva para que o tratamento de dados pessoais seja legítimo. Estes requisitos aplicam-se, além da aplicação do artigo 5.º, n.º 3, a algumas destas partes interessadas quando o tratamento em causa vai além do

armazenamento de informação ou da obtenção de acesso a informação armazenada no equipamento terminal do utilizador/assinante[21].

Na prática, são relevantes três bases jurídicas neste contexto.

O consentimento (artigo 7.º, alínea a)) é a primeira base jurídica que deve ser invocada no contexto da IdC, seja pelos fabricantes de dispositivos, pelas plataformas de dados ou sociais, pelos emprestadores de dispositivos ou pelos criadores de aplicações de terceiros. Em várias ocasiões, o Grupo de Trabalho também emitiu orientações sobre a aplicação simultânea dos requisitos do artigo 7.º, alínea a), e do artigo 5.º, n.º 3, da Diretiva 2002/58/CE[22]. As condições para que esse consentimento seja válido nos termos da legislação da UE também foram especificadas num parecer anterior do Grupo de Trabalho[23].

O artigo 7.º, alínea b), também prevê que o tratamento é legítimo quando é necessário para a execução de um contrato em que a pessoa em causa seja parte. O âmbito deste fundamento jurídico é limitado pelo critério da «necessidade», que exige uma ligação direta e objetiva entre o tratamento propriamente dito e as finalidades do desempenho contratual esperado do titular dos dados.

Em terceiro lugar, o artigo 7.º, alínea f), permite o tratamento de dados pessoais sempre que este seja necessário para prosseguir interesses legítimos do responsável pelo tratamento ou do terceiro ou terceiros a quem os dados sejam comunicados, desde que não prevaleçam os interesses ou os direitos e liberdades fundamentais do titular dos dados — em particular, o seu direito à privacidade no que diz respeito ao tratamento de dados pessoais — protegidos ao abrigo do n.º 1 do artigo 1.º da diretiva.

No seu acórdão no processo *Google Spain*[24], o Tribunal de Justiça Europeu forneceu orientações substanciais sobre a interpretação desta disposição, além das já fornecidas nos processos apensos anteriores ASNEF e FECEMD (C-468/10 e C-469/10). No contexto da IdC, o tratamento de dados pessoais de um indivíduo é suscetível de afetar significativamente os seus direitos fundamentais à privacidade e à proteção de dados pessoais nas situações em que, na ausência dispositivos IdC, os seus dados não poderiam ter sido interligados ou apenas o seriam com grande dificuldade. Estas situações podem ocorrer quando os dados recolhidos se referem ao estado de saúde do indivíduo, ao seu lar ou intimidade, à sua localização e a muitos outros aspetos da sua vida privada. À luz da potencial gravidade dessa interferência, é evidente que tal tratamento dificilmente poderá ser justificado apenas pelo interesse económico que uma parte interessada na IdC tenha nele. Devem ser tidos em conta outros interesses perseguidos pelo responsável pelo tratamento ou pelo terceiro ou terceiros a quem os dados são divulgados[25].

---

[21] Sobre a articulação do artigo 5.º, n.º 3, e do artigo 7.º, alínea a), ver, em particular, o Parecer 02/2013 sobre as aplicações em dispositivos inteligentes, adotado em 27 de fevereiro de 2013 (WP 202) – (p. 14 e seguintes) http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_pt.pdf e o Parecer 06/2014 sobre o conceito de interesses legítimos do responsável pelo tratamento dos dados na aceção do artigo 7.º da Diretiva 95/46/CE (WP 217) – (pp. 26, 32 e 46).

[22] Parecer WP 202, p. 14 e seguintes.

[23] Parecer 15/2011 sobre a definição de consentimento, adotado em 3 de julho de 2011 (WP 187), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_pt.pdf

[24] Acórdão do Tribunal de Justiça (Grande Secção), 13 de maio de 2014, processo C-131/12 (número 74 e seguintes).

[25] Parecer WP 217.

Exemplo: no âmbito de um plano para promover a utilização dos transportes públicos e reduzir a poluição, a Câmara Municipal pretende regular o estacionamento no centro da cidade através da imposição de restrições de acesso, bem como de taxas de estacionamento. O montante da taxa depende de vários parâmetros, incluindo o tipo de motor (gasóleo, gasolina, elétrico) e a idade do veículo. Assim que um veículo se aproxima de um lugar de estacionamento livre, um sensor pode ler a matrícula a fim de determinar, após verificação numa base de dados, o custo adicional ou desconto a ser aplicado automaticamente de acordo com critérios predefinidos. Neste caso, o tratamento da informação da matrícula para determinar a taxa pode satisfazer o interesse legítimo do responsável pelo tratamento. Outros tratamentos, como a obtenção de informações – não anonimizadas – sobre a circulação de veículos na área restrita, exigiria o recurso a outra base jurídica.

4.3 **Princípios relativos à qualidade dos dados**

No seu conjunto, os princípios consagrados no artigo 6.º da Diretiva 95/4/CE constituem a pedra angular da legislação da UE relativa à proteção de dados.

Os dados pessoais devem ser recolhidos e tratados de modo leal e lícito. O princípio da lealdade exige especificamente que os dados pessoais nunca sejam recolhidos e tratados sem o conhecimento do indivíduo. Este requisito é ainda mais importante em relação à IdC, uma vez que os sensores são concebidos para serem discretos, ou seja, para serem o mais invisíveis possível. No entanto, os responsáveis pelo tratamento que atuam na IdC (principalmente os fabricantes de dispositivos) devem informar todos os indivíduos na proximidade geográfica ou digital dos dispositivos conectados sempre que são recolhidos dados relativos a eles ou ao ambiente onde se encontram. O cumprimento desta disposição vai além de um requisito legal estrito: a recolha leal diz respeito às expectativas mais cruciais do utilizador em relação à IdC, em especial no que diz respeito à computação vestível.

Exemplo: um dispositivo relacionado com a saúde utiliza uma pequena luz para monitorizar a circulação do sangue nas veias e para reencaminhar informações sobre os batimentos cardíacos. O dispositivo inclui um outro sensor que mede o nível de oxigénio no sangue, contudo não estão disponíveis informações acerca desta recolha de dados no dispositivo nem na interface do utilizador. Mesmo que o sensor de oxigénio no sangue esteja plenamente funcional, não deve ser ativado sem se informar previamente o utilizador. Será necessário consentimento explícito para ativar este sensor.

O princípio da limitação da finalidade implica que os dados só podem ser recolhidos para fins específicos, explícitos e legítimos. Qualquer outro tratamento incompatível com esses fins iniciais seria ilegal ao abrigo da legislação da UE. Este princípio visa permitir aos utilizadores saber como e para que fins os seus dados serão utilizados e decidir se devem confiá-los a um responsável pelo tratamento. Estes fins devem ser definidos *antes* de ocorrer o tratamento de dados, o que exclui alterações repentinas nas condições fundamentais do tratamento. Tal implica que as partes interessadas na IdC tenham uma boa panorâmica do seu projeto antes de começarem a recolher dados pessoais.

Além disso, os dados recolhidos sobre o titular dos dados devem ser os estritamente necessários para os fins específicos previamente determinados pelo responsável pelo tratamento (princípio da «minimização dos dados»). Os dados que sejam desnecessários para esse fim não devem ser recolhidos e armazenados «para qualquer eventualidade» ou porque «podem vir a ser úteis». Algumas partes interessadas consideram que o princípio da minimização dos dados pode limitar potenciais oportunidades da IdC e, por conseguinte, constituir um obstáculo à inovação, com base na ideia de que os potenciais benefícios do tratamento de dados viriam de uma análise exploratória destinada a

encontrar tendências e correlações não evidentes. O Grupo de Trabalho não pode partilhar desta análise e insiste que o princípio da minimização dos dados desempenha um papel essencial na salvaguarda dos direitos de proteção de dados concedidos pela legislação da UE aos indivíduos, pelo que devem ser respeitados enquanto tal[26]. Este princípio implica especificamente que, quando os dados pessoais não são necessários para prestar um serviço específico na IdC, o interessado deve, pelo menos, ter a possibilidade de utilizar o serviço de forma anónima.

O artigo 6.º também exige que os dados pessoais recolhidos e tratados no contexto da IdC sejam conservados apenas durante o período necessário para a prossecução das finalidades para que foram recolhidos ou para que são tratados posteriormente. Este teste de necessidade deve ser realizado por todas as partes interessadas na prestação de um serviço específico na IdC, uma vez que as finalidades do seu tratamento podem, de facto, ser diferentes. Por exemplo, os dados pessoais comunicados por um utilizador quando assina um serviço específico na IdC devem ser apagados logo que o utilizador ponha termo à sua assinatura. Do mesmo modo, quaisquer informações apagadas pelo utilizador da sua conta não devem ser conservadas. Quando um utilizador não utiliza o serviço ou a aplicação por um período de tempo definido, o perfil de utilizador deve ser definido como inativo. Após um outro período de tempo, os dados devem ser apagados. O utilizador deve ser notificado antes de serem tomadas estas medidas, com todos os meios que a parte interessada em causa tiver à sua disposição.

4.4 **Tratamento de dados sensíveis (artigo 8.º)**

As aplicações na IdC podem efetuar o tratamento de dados pessoais suscetíveis de revelar a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, a filiação sindical ou informações sobre a saúde ou a vida sexual, o que efetivamente se qualifica como «dados sensíveis», que merecem uma proteção especial na aceção do artigo 8.º da Diretiva 95/46/CE. Na prática, a aplicação do artigo 8.º aos dados sensíveis na IdC exige que os responsáveis pelo tratamento obtenham o consentimento explícito do utilizador, a menos que o próprio titular dos dados os tenha divulgado publicamente.

Esta situação pode surgir em contextos específicos, como nos dispositivos de eu quantificado. Nestes casos, os dispositivos relevantes registam sobretudo dados relativos ao bem-estar do indivíduo. Estes dados não constituem, necessariamente, dados de saúde enquanto tal, no entanto podem rapidamente fornecer informações sobre a saúde do indivíduo, uma vez que registam a hora em que são recolhidos, tornando possível retirar ilações da sua variabilidade ao longo de um determinado período. Os responsáveis pelo tratamento devem prever esta eventual mudança na qualificação e tomar medidas adequadas em conformidade.

Exemplo: a empresa X desenvolveu uma aplicação que, através da análise de dados brutos de sinais de eletrocardiogramas gerados por sensores comerciais vulgarmente disponíveis aos consumidores, é capaz de detetar padrões de toxicodependência. O mecanismo da aplicação consegue extrair características específicas dos dados brutos do ECG que, de acordo com resultados de estudos anteriores, estão ligadas ao consumo de droga. O produto, compatível com a maior parte dos sensores existentes no mercado, poderia ser utilizado como uma aplicação independente ou através de uma interface web que requeira o carregamento dos dados. Deve ser obtido o consentimento explícito do

[26] Em qualquer caso, na prática a investigação exploratória nunca é realizada de forma aleatória: o objetivo geral de qualquer investigação é tradicionalmente definido, pelo menos parcialmente, nem que seja apenas por razões organizacionais e orçamentais. É difícil imaginar que o tratamento de dados para uma investigação específica seja compatível com a finalidade inicial da recolha de dados e, por conseguinte, entra em conflito com a legislação da UE.

utilizador para tratar os dados para esse fim. A conformidade com este requisito de consentimento pode ser cumprida nas mesmas condições e ao mesmo tempo em que é obtido o consentimento do titular dos dados nos termos do artigo 7.º, alínea a).

4.5 **Requisitos de transparência (artigos 10.º e 11.º)**

Para além da exigência de recolha leal dos dados prevista no artigo 6.º, alínea a), os responsáveis pelo tratamento devem comunicar informações específicas ao titular dos dados, em aplicação dos artigos 10.º e 11.º: a identidade do responsável pelo tratamento, as finalidades do tratamento, os destinatários dos dados, a existência dos seus direitos de acesso e do direito de oposição (que inclui informações sobre como desligar o objeto para impedir a divulgação de outros dados).

Consoante as aplicações, esta informação pode ser fornecida, por exemplo, no próprio objeto, utilizando a conectividade sem fios para transmitir as informações, ou através da localização por meio de um teste de proximidade preservador da privacidade feito por um servidor centralizado para informar os utilizadores de que estão localizados perto do sensor.

Estas informações devem ainda ser fornecidas de forma clara e compreensível, em conformidade com o princípio do tratamento leal dos dados. Por exemplo, o fabricante de dispositivos pode imprimir um código QR nas coisas equipadas com sensores, ou um *flashcode* que descreva o tipo de sensores e a informação que capta, bem como as finalidades destas recolhas de dados.

4.6 **Segurança (artigo 17.º)**

O artigo 17.º da Diretiva Proteção de Dados estabelece que o responsável pelo tratamento «*deve pôr em prática medidas técnicas e organizativas adequadas para proteger os dados pessoais*» e que *«o responsável pelo tratamento, em caso de tratamento por sua conta, deverá escolher um subcontratante que ofereça garantias suficientes em relação às medidas de segurança técnica e de organização do tratamento a efetuar»*.

Por conseguinte, qualquer parte interessada que se qualifique como responsável pelo tratamento continua a ser plenamente responsável pela segurança do tratamento de dados. Se as falhas de segurança que resultem na violação do princípio da segurança forem consequência de uma conceção ou manutenção inadequadas dos dispositivos utilizados, é ativada a responsabilidade do responsável pelo tratamento. Nesse sentido, é necessário que estes responsáveis pelo tratamento realizem avaliações de segurança dos sistemas na sua globalidade, incluindo ao nível dos componentes, aplicando os princípios da segurança agregada. Na mesma linha, deve ser implementada a utilização de certificação para os dispositivos, bem como o alinhamento com as normas de segurança internacionalmente reconhecidas, para melhorar a segurança global do ecossistema da IdC.

Os subcontratantes que concebem e fabricam componentes de *hardware* por conta de outras partes interessadas sem efetivamente efetuarem o tratamento de dados pessoais não podem, em rigor, ser responsabilizados nos termos do artigo 17.º da Diretiva 95/46/CE caso ocorra uma violação da proteção de dados devido a uma falha na segurança desses dispositivos. Ainda assim, estas partes interessadas desempenham um papel fundamental na manutenção da segurança do ecossistema da IdC. As partes interessadas que são diretamente responsáveis perante os titulares dos dados no que diz respeito à proteção de dados devem certificar-se de que esses subcontratantes aplicam efetivamente elevados padrões de segurança em matéria de privacidade aquando da conceção e do fabrico dos seus produtos.

Tal como foi referido antes, as medidas de segurança devem ser postas em prática tendo em conta os condicionalismos operacionais específicos dos dispositivos IdC. Por exemplo, hoje em dia, a maioria dos sensores não é capaz de estabelecer uma ligação encriptada devido à prioridade que é dada à autonomia física do dispositivo ou ao controlo dos custos.

Além disso, os dispositivos que operam na IdC também são difíceis de proteger, tanto por motivos técnicos como comerciais. Dado que os seus componentes utilizam, geralmente, uma infraestrutura de comunicação sem fios e se caracterizam por disporem de recursos limitados em termos de energia e capacidade de processamento, os dispositivos são vulneráveis a ataques físicos, espionagem ou ataques por *proxy*. As tecnologias atualmente mais utilizadas – ou seja, as infraestruturas de chave pública (PKI – *Public Key Infrastructures*) – não são transferidas facilmente para os dispositivos IdC, uma vez que a maior parte dos dispositivos não tem a capacidade de processamento necessária para lidar com as tarefas de processamento exigidas. A IdC implica uma cadeia de abastecimento complexa em que múltiplas partes interessadas assumem diferentes graus de responsabilidade. Uma quebra de segurança pode ter origem em qualquer uma delas, especialmente quando se tem em conta os ambientes M2M baseados no intercâmbio de dados entre dispositivos. Por conseguinte, deve ser tida em conta a necessidade de recorrer a protocolos seguros e leves que possam ser utilizados em ambientes com poucos recursos.

Neste contexto, em que a reduzida capacidade de processamento pode colocar em risco a comunicação segura e eficiente, o Grupo de Trabalho salienta que é ainda mais importante respeitar o princípio de minimização dos dados e restringir ao mínimo necessário o tratamento de dados pessoais, em especial o seu armazenamento nos dispositivos.

Além disso, os dispositivos concebidos para serem acedidos diretamente através da Internet nem sempre são configurados pelo utilizador. Podem, por conseguinte, proporcionar um canal de acesso fácil a intrusos se continuarem a funcionar com as configurações predefinidas. As práticas de segurança baseadas em restrições de rede, que desativam por predefinição funcionalidades não críticas e que impedem a utilização de fontes de atualização de *software* não fidedignas (limitando assim os ataques de vírus malévolos baseados na alteração de código) poderiam contribuir para limitar o impacto e a extensão de eventuais violações de dados. Estas proteções da privacidade devem ser incorporadas desde o início, em aplicação do princípio da «privacidade desde a conceção».

Além disso, a ausência de atualizações automáticas resulta em frequentes vulnerabilidades não corrigidas que podem facilmente ser descobertas por meio de motores de busca especializados. Mesmo nos casos em que os utilizadores têm conhecimento das vulnerabilidades que afetam os seus dispositivos, podem não ter acesso às atualizações do vendedor, seja devido a limitações do *hardware* ou a tecnologias desatualizadas que impedem que o dispositivo suporte atualizações de *software*. Caso um fabricante de dispositivos deixe de dar assistência a um dispositivo, devem ser fornecidas soluções alternativas de apoio (por exemplo, abrir o *software* à comunidade de fonte aberta). Os utilizadores devem ser notificados de que os seus dispositivos são suscetíveis de se tornarem vulneráveis a falhas não corrigidas.

Alguns dos sistemas de automonitorização (por exemplo, pedómetros, monitorizadores de sono) existentes no mercado também sofrem de falhas de segurança que permitem a atacantes adulterar os valores observados que são comunicados às aplicações e aos fabricantes de dispositivos. É essencial que estes dispositivos ofereçam proteções adequadas contra a adulteração de dados, em especial se os

valores comunicados por estes sensores afetarem indiretamente as decisões dos utilizadores em matéria de saúde.

Por último, mas não menos importante, uma política adequada de notificação de violações de dados pode também ajudar a conter os efeitos negativos das vulnerabilidades de *software* e de conceção ao difundir conhecimentos e proporcionar orientação sobre essas questões.

5. Direitos dos titulares de dados

As partes interessadas na IdC devem respeitar os direitos dos titulares de dados nos termos do disposto nos artigos 12.º e 14.º da Diretiva 95/46/CE e tomar medidas organizativas em conformidade. Estes direitos não são limitados aos assinantes de serviços IdC ou a proprietários de dispositivos e dizem respeito a qualquer indivíduo cujos dados pessoais sejam objeto de tratamento.

5.1 **Direito de acesso**

O artigo 12.º, alínea a), prevê que os titulares dos dados têm o direito de obter dos responsáveis pelo tratamento a comunicação, numa forma inteligível, dos dados que são submetidos a tratamento e de todas as informações disponíveis sobre a sua fonte.

Na prática, os utilizadores na IdC tendem a estar presos a sistemas específicos. Normalmente, os dispositivos enviam, em primeiro lugar, dados ao fabricante do dispositivo que, em seguida, torna estes dados acessíveis ao utilizador através de um portal na Internet ou de uma aplicação. Esta conceção permite aos fabricantes prestar serviços em linha que aproveitam as capacidades do dispositivo, mas também pode impedir os utilizadores de escolherem livremente o serviço que pretendem que interaja com o seu dispositivo.

Além disso, hoje em dia, os utilizadores finais raramente estão em condições de aceder aos dados brutos que são registados pelos dispositivos IdC. Claramente, possuem um interesse mais imediato nos dados interpretados do que nos dados brutos, que para eles podem não fazer sentido. Ainda assim, o acesso a esses dados pode ser útil para os utilizadores finais entenderem o que o fabricante de dispositivos pode, a partir deles, inferir a seu respeito. Além disso, beneficiar destes dados brutos dar-lhes-ia a capacidade para transferir os seus dados para outro responsável pelo tratamento e mudar de serviços, por exemplo se o responsável pelo tratamento inicial fizesse alterações à sua política de privacidade com as quais não concordassem. Hoje em dia, na prática, essas pessoas não têm outra possibilidade para além de interromper a utilização dos seus dispositivos, uma vez que a maior parte dos responsáveis pelo tratamento não fornece esse tipo de funcionalidade e apenas concede acesso a uma versão dos dados brutos armazenados de má qualidade.

O Grupo de Trabalho considera que tais comportamentos impedem o exercício efetivo do direito de acesso concedido aos indivíduos pelo artigo 12.º, alínea a), da Diretiva 95/46/CE. Considera que, pelo contrário, as partes interessadas na IdC devem tomar medidas que permitam efetivamente aos utilizadores fazer valer esse direito e oferecer aos utilizadores a possibilidade de optar por um outro serviço que possa não ser proposto pelo fabricante do dispositivo. Normas relativas à interoperabilidade dos dados poderiam ser desenvolvidas para esse efeito.

A pertinência destas medidas é, além disso, reforçada pelo facto de o chamado «direito de portabilidade», que o projeto de regulamento geral de proteção de dados irá, provavelmente, consagrar como uma variante do direito de acesso, pretender colocar um fim claro a situações de «prisão» do

utilizador[27]. A ambição do legislador europeu relativamente a este aspeto consiste em desbloquear os impedimentos à concorrência e ajudar novos intervenientes a inovar neste mercado.

5.2 **Possibilidade de retirar o consentimento e de se opor**

Os titulares de dados devem ter a possibilidade de revogar qualquer consentimento dado previamente para um tratamento de dados específico e de se opor ao tratamento de dados que lhes digam respeito. O exercício de tais direitos deve ser possível sem quaisquer restrições técnicas ou organizativas e sem obstáculos, enquanto os instrumentos fornecidos para registar essa revogação devem ser acessíveis, visíveis e eficientes.

Os regimes de revogação devem ser detalhados e devem abranger: (1) quaisquer dados recolhidos por uma coisa específica (por exemplo, requerer que a estação meteorológica pare de recolher dados relativos à humidade, à temperatura e aos sons); (2) um tipo específico de dados recolhidos por qualquer coisa (por exemplo, um utilizador deve poder interromper a recolha de dados por qualquer dispositivo de gravação de som, seja um monitorizador de sono ou uma estação meteorológica); (3) um tratamento de dados específico (por exemplo, um utilizador pode exigir que tanto o seu pedómetro como o seu relógio parem de contar os seus passos).

Além disso, uma vez que é provável que as «coisas conectadas» vestíveis venham a substituir objetos existentes que oferecem funcionalidades comuns, os responsáveis pelo tratamento devem oferecer a opção de desativar a função «conectada» da coisa e permitir que ela funcione como um objeto original, não conectado (ou seja, desativar a funcionalidade conectada do relógio ou dos óculos inteligentes). O Grupo de Trabalho já especificou que os titulares de dados devem ter a possibilidade de «anular a cada momento o seu consentimento, sem ter de fechar a aplicação»[28].

Exemplo: um utilizador instala um alarme de incêndios conectado no seu apartamento. O alarme utiliza um sensor de presença, um sensor de calor, um sensor de ultrassons e um sensor de luz. Alguns destes sensores são necessários para detetar incêndios, ao passo que outros apenas fornecem funcionalidades adicionais sobre as quais o utilizador foi previamente informado. O utilizador deve ser capaz de desativar estas funcionalidades a fim de fazer uso apenas do alarme de incêndios e, por conseguinte, desligar os sensores que oferecem essas funcionalidades.

Curiosamente, alguns desenvolvimentos recentes neste domínio estão a tentar capacitar os titulares de dados, dando-lhes mais controlo sobre as funcionalidades de gestão do consentimento, nomeadamente através da utilização de *sticky policies*[29] ou *proxies* para privacidade[30].

---

[27] http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_pt.pdf

[28] Parecer 13/2011 sobre serviços de geolocalização em dispositivos móveis inteligentes, adotado em 16 de maio de 2011 (WP 185) - http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp185_pt.pdf

[29] A este respeito, a utilização de uma abordagem baseada nas chamadas *sticky policies* pode apoiar a conformidade com o quadro de proteção de dados ao incluir informações sobre as condições e os limites à utilização de dados juntamente com os próprios dados. Por conseguinte, estas políticas poderiam estabelecer o contexto da utilização dos dados, as finalidades, as políticas de acesso de terceiros e uma lista de utilizadores de confiança.

[30] Uma forma de oferecer ao titular dos dados um controlo real sobre o modo como os dados devem ser tratados quando interagem com sensores através da possibilidade de manifestar as suas preferências, incluindo de obter e revogar o consentimento e de fazer escolhas de limitação da finalidade, poderia basear-se na utilização de

6. Conclusões e recomendações

Segue-se uma série de recomendações que o Grupo de Trabalho do artigo 29.º considerou úteis para facilitar a aplicação dos requisitos legais da UE em matéria de IdC supramencionados.

As recomendações que a seguir se formulam fornecem apenas uma orientação que suplementa os documentos anteriormente adotados pelo Grupo de Trabalho.

A este respeito, o Grupo de Trabalho deseja chamar especificamente a atenção para as suas recomendações anteriores sobre as aplicações em dispositivos inteligentes[31]. Dado que os *smartphones* fazem parte do ambiente da IdC e que ambos os ecossistemas envolvem um conjunto comparável de partes interessadas, estas recomendações são diretamente relevantes para a IdC. Em especial, os criadores de aplicações e os fabricantes de dispositivos devem fornecer um nível adequado de informação aos utilizadores finais e oferecer autoexclusões (*opt-outs*) simples e/ou consentimento diferenciado, se for caso disso. Além disso, quando o consentimento não tiver sido obtido, o responsável pelo tratamento deve tornar os dados anónimos antes de redefinir a sua finalidade ou de os partilhar com outras partes.

6.1 Recomendações comuns a todas as partes interessadas

- Antes de serem lançadas quaisquer novas aplicações na IdC, devem ser realizadas avaliações do impacto sobre a privacidade (PIA). A metodologia a adotar para essas PIA pode basear-se no quadro para as avaliações do impacto na proteção da privacidade e dos dados, que o Grupo de Trabalho adotou em 12 de janeiro de 2011 para as aplicações RFID[32]. Sempre que adequado/possível, as partes interessadas devem ponderar disponibilizar a PIA relevante ao público em geral. Poderiam ser desenvolvidos quadros específicos para PIA adaptados a determinados ecossistemas IdC (por exemplo, cidades inteligentes).

- Muitas partes interessadas na IdC apenas necessitam de dados agregados e não precisam dos dados brutos recolhidos pelos dispositivos IdC. As partes interessadas devem apagar os dados brutos logo que tenham extraído os dados necessários para o seu tratamento de dados. Por princípio, essa eliminação dos dados deve ocorrer o mais próximo possível da recolha de dados brutos (por exemplo, no mesmo dispositivo após o tratamento).

- Todas as partes interessadas na IdC devem aplicar os princípios da privacidade desde a conceção e da privacidade por predefinição.

- A capacitação do utilizador é essencial no contexto da IdC. Os titulares de dados e os utilizadores devem poder exercer os seus direitos e, por conseguinte, «deter o controlo» dos dados a todo o momento, de acordo com o princípio da autodeterminação dos dados.

- As modalidades para prestar as informações e proporcionar o direito de recusar ou solicitar consentimento devem ser tão conviviais quanto possível. Em especial, as políticas de informação e

---

proxies para privacidade. Apoiados por um dispositivo, os pedidos de dados são confrontados com políticas predefinidas que regem o acesso aos dados sob o controlo do seu titular. Ao definir pares de sensores e políticas, os pedidos de terceiros de recolha ou acesso aos dados dos sensores seriam autorizados, limitados ou simplesmente rejeitados.

[31] Parecer 02/2013 sobre as aplicações em dispositivos inteligentes (WP 202), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_pt.pdf

[32] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_annex_en.pdf

consentimento devem centrar-se em informações que sejam compreensíveis para o utilizador e não devem limitar-se a uma política geral de privacidade no sítio Web dos responsáveis pelo tratamento.

- Os dispositivos e aplicações devem igualmente ser concebidos de modo a informarem os utilizadores e os titulares dos dados não utilizadores, por exemplo através da interface física do dispositivo ou da transmissão de um sinal num canal sem fios.

6.2 **O sistema operativo e os fabricantes de dispositivos**

- Os fabricantes de dispositivos devem informar os utilizadores sobre o tipo de dados que são recolhidos pelos sensores e posteriormente tratados, sobre os tipos de dados que recebem e sobre o modo como vão ser tratados e combinados.

- Os fabricantes de dispositivos devem poder comunicar, de imediato, a todas as outras partes interessadas envolvidas sempre que um titular de dados retire o seu consentimento ou se oponha ao tratamento dos dados.

- Os fabricantes de dispositivos devem facultar escolhas diferenciadas quando concedem acesso a aplicações. A diferenciação não deve apenas dizer respeito à categoria de dados recolhidos, mas também ao tempo e à frequência com que os dados são recolhidos. À semelhança da funcionalidade «não incomodar» existente nos *smartphones*, os dispositivos IdC devem oferecer uma opção de «não recolher» para programar ou desativar rapidamente os sensores.

- Para evitar a monitorização da localização geográfica, os fabricantes de dispositivos devem limitar a recolha de impressões digitais do dispositivo desativando as interfaces sem fios quando não estejam a ser utilizadas, ou devem utilizar identificadores aleatórios (tais como endereços MAC aleatórios para varrer redes Wi-Fi), a fim de evitar a utilização de um identificador persistente para monitorização da localização.

- A fim de assegurar a transparência e o controlo do utilizador, os fabricantes de dispositivos devem fornecer ferramentas que permitam ler, editar e alterar os dados localmente, antes de estes serem transferidos para o responsável pelo tratamento. Além disso, os dados pessoais tratados por um dispositivo devem ser armazenados num formato que permita a portabilidade dos dados.

- Os utilizadores têm o direito de aceder aos seus dados pessoais. Devem ser-lhes fornecidas ferramentas que lhes permitam exportar facilmente os seus dados num formato estruturado e vulgar. Por conseguinte, os fabricantes de dispositivos devem fornecer uma interface convivial aos utilizadores que pretendam obter dados agregados e/ou dados brutos que ainda armazenem.

- Os fabricantes de dispositivos devem facultar ferramentas simples para notificar os utilizadores e atualizar os dispositivos quando são detetadas vulnerabilidades de segurança. Quando um dispositivo se torna obsoleto e deixa de ser atualizado, o fabricante de dispositivos deve notificar o utilizador e certificar-se de que este tem conhecimento de que o dispositivo deixará de ser atualizado. Todas as partes interessadas suscetíveis de serem afetadas pela vulnerabilidade em causa devem também ser informadas.

- Os fabricantes de dispositivos devem seguir um processo de «segurança desde a conceção» e dedicar alguns componentes às principais primitivas criptográficas.

- Os fabricantes de dispositivos devem limitar, tanto quanto possível, a quantidade de dados que sai dos dispositivos transformando os dados brutos em dados agregados diretamente no dispositivo. Os dados agregados devem estar num formato normalizado.

- Ao contrário dos *smartphones*, os dispositivos IdC podem ser partilhados por vários titulares de dados ou podem ser mesmo alugados (por exemplo, casas inteligentes). Deve estar disponível uma configuração que permita distinguir entre indivíduos diferentes que utilizam o mesmo dispositivo, para que não tomem conhecimento das atividades uns dos outros.

- Os fabricantes de dispositivos devem trabalhar com os organismos de normalização e com as plataformas de dados para apoiar um protocolo comum que permita manifestar preferências no que se refere à recolha e ao tratamento de dados pelos responsáveis pelo tratamento, em particular quando esses dados são recolhidos por dispositivos discretos.

- Os fabricantes de dispositivos devem autorizar entidades de controlo e de tratamento locais (os chamados *proxies* de privacidade pessoais), que permitem que os utilizadores tenham uma panorâmica clara dos dados recolhidos pelos seus dispositivos e facilitam o armazenamento e o tratamento locais sem terem de transmitir os dados ao fabricante de dispositivos.

6.3 **Criadores de aplicações**

- Devem ser concebidos avisos ou notificações para lembrar frequentemente os utilizadores de que os sensores estão a recolher dados. Quando o criador da aplicação não tem acesso direto ao dispositivo, a aplicação deve enviar periodicamente uma notificação ao utilizador a informá-lo de que ainda está a registar dados.

- As aplicações devem facilitar o exercício pelo titular dos dados dos direitos de acesso, alteração e eliminação de informações pessoais recolhidas pelos dispositivos IdC.

- Os criadores de aplicações devem facultar ferramentas que permitam aos titules de dados exportar dados agregados e/ou brutos num formato normalizado e utilizável.

- Os criadores devem prestar especial atenção aos tipos de dados que são tratados e à possibilidade de se extraírem dados pessoais sensíveis a partir deles.

- Os criadores de aplicações devem aplicar o princípio de minimização dos dados. Sempre que a finalidade puder ser alcançada através da utilização de dados agregados, os criadores não devem aceder aos dados brutos. De um modo mais geral, os criadores devem seguir uma abordagem de «privacidade desde a conceção» e minimizar a quantidade de dados recolhidos à necessária para prestar o serviço.

6.4 **Plataformas sociais**

- As configurações predefinidas das aplicações sociais baseadas em dispositivos IdC devem solicitar aos utilizadores que revejam, editem e decidam quanto à informação gerada pelo seu dispositivo antes da publicação em plataformas sociais.

- As informações publicadas pelos dispositivos IdC em plataformas sociais não devem, por predefinição, tornar-se públicas ou ser indexadas por motores de busca.

6.5 **Proprietários de dispositivos IdC e outros destinatários**

- O consentimento na utilização de um dispositivo conectado e no tratamento de dados subsequente deve ser informado e concedido livremente. Os utilizadores não devem ser penalizados economicamente nem ter um acesso de pior qualidade às capacidades dos seus dispositivos se decidirem que não pretendem utilizar o dispositivo ou um serviço específico.

- O interessado cujos dados são tratados no contexto de uma relação contratual com o utilizador de um dispositivo conectado (ou seja, hotel, seguro de doença ou serviço de aluguer de automóveis), deve estar em condições de administrar o dispositivo. Independentemente da existência de uma relação contratual, qualquer titular de dados não utilizador deve ser capaz de exercer os seus direitos de acesso e de oposição.

- Os utilizadores de dispositivos IdC devem informar os titulares de dados não utilizadores cujos dados são recolhidos, acerca da presença de dispositivos IdC e do tipo de dados recolhidos. Devem também respeitar a preferência dessa pessoa de que os seus dados não sejam recolhidos pelo dispositivo.

6.6 **Organismos de normalização e plataformas de dados**

- Os organismos de normalização e as plataformas de dados devem promover formatos de dados portáteis e interoperáveis, bem como formatos de dados claros e autoexplicativos, a fim de facilitar as transferências de dados entre diferentes partes e de ajudar os titulares dos dados a entenderem quais os dados que estão efetivamente a ser recolhidos sobre eles pelos dispositivos IdC.

- Os organismos de normalização e as plataformas de dados não devem centrar-se apenas no formato para dados brutos, mas também na emergência de formatos para dados agregados.

- Os organismos de normalização e as plataformas de dados devem promover formatos de dados que contenham o mínimo possível de identificadores fortes, a fim de facilitar a anonimização adequada dos dados IdC.

- Os organismos de normalização devem trabalhar na elaboração de normas certificadas que estabeleçam a linha de base para a salvaguarda da segurança e da privacidade dos titulares de dados.

- Os organismos de normalização devem desenvolver protocolos leves de encriptação e comunicação adaptados às especificidades da IdC, garantindo a confidencialidade, a integridade, a autenticação e o controlo do acesso.