SINERGIA NA RESOLUÇÃO DE LITÍGOS EM LINHA E A NECESSIDADE DE PROTEÇÃO DA PRIVACIDADE E DOS DADOS PESSOAIS

SYNERGY IN ONLINE DISPUTE RESOLUTION AND THE NEED TO PROTECT PRIVACY AND PERSONAL DATA

Cristiana Santos[1], Francisco Andrade[2], Paulo Novais[3]

Artigo recebido em 25 mar. 2014 e aceito em 22 abr. 2014.

Resumo

Esta contribuição apresenta uma nova compleição para a resolução de litígios em linha. Neste artigo pretendemos aferir se a performatividade e sinergia dos sistemas de Ambiente Inteligente (AmI), através da inserção de sensores introduzidos em dispositivos móveis que nos são familiares, poderá enriquecer o processo comunicacional e decisional na resolução de conflitos em linha. Com estes novos contributos, fornecemos uma perspectiva das principais implicações jurídicas do uso desta tecnologia de natureza ubíqua no ODR. Propomo-nos a retratar e responder às principais críticas e apreensões relacionadas com o AmI e conceituamo-las no quadrante da mediação online. Dispomo-nos a analisar a relevância, aplicabilidade e adequação da legislação atinente à privacidade e proteção de dados face aos emergentes desafios do AmI.

Palavras-chave
ODR. Ambiente Inteligente. Informação Contextual. Privacidade e Proteção de Dados. Regulação.

[1] Mestre em Direito dos Contratos e Empresa pela Universidade do Minho (UMINHO). Doutoranda bolseira pelo Instituto de Direito e Tecnologia da Universidade Autónoma de Barcelona (UAB) e doutoranda pelo Joint International Doctoral (Ph.D.). Barcelona, Catalunha, Espanha. E-mail: cristiana.teixeirasantos@gmail.com

[2] Doutor em Direito pela Universidade do Minho (UMINHO). Professor Auxiliar da Escola de Direito da Universidade do Minho (UMINHO). Braga, Portugal. E-mail: fandrade@direito.uminho.pt

[3] Doutor em Informática pela Universidade do Minho (UMINHO). Professor Associado com Agregação do Departamento de Informática da Universidade do Minho (UMINHO). Braga, Portugal. E-mail: pjon@di.uminho.pt

Abstract

This contribution presents a new approach to online dispute resolution. In this article we aim to assess whether the synergy and the performativity of Ambient Intelligent Systems (AmI), by inserting sensors in mobile devices that are familiar to us, can enhance the communication and the decision-making process in online dispute resolution. With these new contributions, we provide a perspective of the main legal implications of using this ubiquitous technology in ODR. We will portray the main criticisms and concerns addressed to Ambient Intelligence and we conceptualize them in the prism of online mediation. We will examine the relevance, applicability and adequacy of privacy and data protection legislation in the prospect of the emerging challenges of AmI.

Keywords
ODR. Ambient Intelligence. Contextual Information.Privacy. Data Protection. Regulation.

1 Introdução

A investigação dominante aponta que a mediação, como método consensual de resolução de conflitos, parece ser particularmente adequada a gerir e resolver conflitos de consumo conforme um estudo representativo constante do Libro Blanco de la Mediación en Catalunya (POBLET et al., 2011). Mas a resolução de litígios em linha pretende-se adaptada às estratégias em tempo real de acordo com as mudanças dos estilos conflituais das partes (CARNEIRO et al., 2011), isto é, através de métodos de resolução que incorporem um ambiente contextual proativo (BROEKENS; JONKER; MEYER, 2010, p.121) das partes em disputa. Referimo-nos ao modelo dotado de um ambiente inteligente, que suporta o ciclo de vida do conflito, e aporta conhecimento contextual importante, capaz de reagir a mudanças no contexto de interação (*context information*), o que resulta numa abordagem de resolução de controvérsias capaz de perceber as partes, alterar estratégias de atuação e, consequentemente, alcançar melhores resultados.

A performatividade dos sistemas de inteligência ambiente parece aportar maior riqueza e apoio à resolução de litígios em linha (FRIEDEWALD et al., 2006). Relacionada com a grande revolução tecnológica da "Internet das Coisas" (ou *Internet of Things,* ou a mais recente, *"internet of everything"*)[4], define-se como a tecnologia dotada de capacidade[5] e poder

[4]Esta relação conceitua-se como "Internet das Coisas" ou "Ambiente Inteligente" (doravante designado de AmI), também denominada na sua sinonímia pelos termos de "computação ubíqua", "generalizada" (ou "*pervasive*"), "nómada", "móvel", "proativa" e "autónoma". Este novo paradigma de futuro constitui um ecossistema tecnológico complexo, exigindo pouca intervenção e deliberação humana e abrange uma ampla gama de diferentes tecnologias emergentes, tais como sensores móveis, identificação por radiofrequência (RFID), agentes de software, implantes de TIC,

de processamento computacional e aportada de dispositivos observáveis e externos (écrans tácteis, câmaras de vídeo, acelerómetros, PDA's, entre outros dispositivos). Estas tecnologias captam informação do ambiente, ou informação contextual, de forma a ser processada para, posteriormente, responder às necessidades dos seus utilizadores.

Neste advento, partimos de um paradigma de ferramentas de comunicação colaborativas e utilizadas pelas partes para partilhar informação, para emergir num ambiente inteligente dotado de conhecimento relevante.[6] Sempre que a plataforma de resolução de conflitos detecta uma mudança significativa (a nível de stress e de saturação, de linguagem corporal e do estado emocional – informação de contexto captada), existe uma adaptação da estratégia. A adaptação de estratégias consiste em mudar a lista de resultados a ser proposta às partes.

Considera-se ainda o uso de informações, por exemplo, pela repetição, intensidade e/ou acuidade no teclar das partes, a fim de determinar o nível de nervosismo, bem como algumas características linguísticas e semânticas, de imagem, análise do discurso, captáveis

computação afetiva e nanotecnologia. Além disso, o cenário de ambiente inteligente baseia-se na construção automática de perfis e na entronização, isto é, a partir da qual os componentes computadorizados ou interfaces intuitivos e inteligentes passam a compor o ambiente e os objetos do quotidiano. Essas tecnologias e dispositivos computadorizados são dotados da capacidade de reconhecer uma determinada pessoa e os seus contextos situacionais, e de responder (adaptando-se e configurando-se) às necessidades dos usuários, antecipando os seus desejos, sem uma imediação consciente, portanto, sem ser percebida. O ambiente também pode e deve ser capaz de detectar outros dispositivos que interajam com ele. Desta conectividade surge a capacidade de os computadores atuarem de forma "inteligente" no ambiente em que o usuário se locomove, sendo esse ambiente saturado por sensores e serviços computacionais. O AmI particulariza-se pela sua invisibilidade, discrição, sensibilidade , interatividade e responsividade à pessoa humana. Ver Weyrich (1999), quem denominou pela 1ª vez o termo de "ambiente inteligente".

[5] Citamos, pelo interesse ilustrativo, o seguinte comentário recente "(...) Por não ser um conceito tão novo quanto possamos pensar, existem já um sem fim de setores nos quais está a ser aplicada esta nova tendência, vejamos o caso da agricultura em que já se começam a usar sensores espalhados pelo terreno para aferir as zonas que mais precisam de fertilizantes. Na área das seguradoras, existe a ideia de associar as apólices não ao perfil do segurado mas sim ao comportamento real de quem conduz o automóvel, registado por vários sensores em tempo real (velocidade, travagens, acidentes, respeito pelos sinais de trânsito e outros). E ainda no ramo automóvel, é possível o automóvel comunicar e fazer diretamente o agendamento da próxima revisão, evitando os problemas mecânicos e garantindo a segurança. Muito se tem falado da utilidade que poderia ser dada à "Internet das Coisas", através da criação de frigoríficos inteligentes que ajudam na gestão dos produtos, alertando sobre os prazos de validade dos alimentos, aprendendo os hábitos de consumo e criando listas de compras que mais tarde só precisariam de uma única validação por parte do utilizador para efetivarem as compras. Este conceito da IoT pode ser aplicado às mais diversas áreas, tem um sem fim de utilidades: pode ajudar a gerir a mais rotineira tarefa do nosso dia-a-dia ou ser perfeitamente utilizado para a gestão, levantamento e reorganização de grandes cidades (...)" (PEREIRA, 2014, *online*).

[6] No entanto, uma das limitações destas configurações de ODR consiste no facto de tais informações de contexto não reproduzirem fielmente o estado atual das partes, mercê de uma distância eletrônica e se encontrarem "escondidas" atrás de uma *interface*.

através de dispositivos não invasivos dotados de sensores de stress, sensores de ambiente, entre outros.

De acordo com as conclusões recentes e aplicações atuais no domínio da resolução de litígios em linha (POBLET; CASANOVAS, 2007, p. 147), as emoções que emergem das interações em linha podem ser identificadas como "funções sociais", "pistas contextuais" ou "índices" (como gestos faciais, inflexão de voz, entonação, entre outros). Esta proposição sugere que a cultura da comunicação online tem parametrizado as suas próprias "pistas paralinguísticas para expressar emoções" (ou seja, por meio de caracteres especiais, emoções, uso de maiúsculas, etc.). Descobertas recentes narram que o ODR não é "emocionalmente limitado" e pode até mitigar grandes apreensões relativas ao facto de se considerar o ODR como dotado de um ambiente impessoal, onde as emoções não podem ser usadas como pistas contextuais ou interativas. As preocupações mais frequentes dos céticos do ODR consistem no facto de os processos online não coincidirem com a riqueza das interações face-a-face; referem que as partes estão mais propensas a experimentarem baixos níveis de confiança interpessoal quando atuam numa base de "écran-a-écran", e suscitam preocupações quanto à confidencialidade, segurança, identidade (HAMMOND, 2003, p. 265). Estudos empíricos concluem que o ODR "permite aos disputantes estarem mais focalizados nas suas interações para avaliarem as suas emoções e expressá-las de forma racional e envolverem-se ao seu próprio ritmo" (POBLET; CASANOVAS, 2007, p. 150). Cognitivamente, postulamos que a resolução de litígios em linha "situa e intensifica a força e o conteúdo do fluxo de comunicação" (CASANOVAS; POBLET; LÓPEZ-COBO, 2011, p. 320).

Caberá à tecnologia sintetizar esta informação contextual e canalizá-la na resolução da disputa. Desta forma, espera-se alcançar mecanismos de resolução de conflitos mais eficientes, capazes de alcançar resultados satisfatórios para as partes. Assim, a tecnologia integrada nos sistemas de ODR deve ser construída de tal forma que os seus intervenientes possam confiar nela como uma forma eficiente e eficaz de gerir as suas disputas (WAHAB, 2004, p. 43). No entanto, esta configuração na resolução de litígios em linha assume características muito próprias. O ambiente inteligente implica um uso/tratamento intensivo de dados pessoais que permite acompanhar tudo o que fazemos. Caracteriza-se pela sua feição invisível (sub-reptícia), em tempo real, polivalente e autónoma no acesso, recolha, armazenamento e processamento de dados. Esta compleição obriga-nos a repensar questões relacionadas com a identidade e autodeterminação da pessoa humana, a privacidade, a proteção de dados, a transparência dos sistemas, o consentimento das partes e a finalidade da recolha de dados, questões que analisaremos neste artigo. Para se alcançar as virtualidades do ambiente inteligente, torna-se compulsório prever e responder a possíveis ameaças emergentes das novas tecnologias perante o "*homo-conectus*" (ANDRADE,

2012), no sentido de fornecer garantias adequadas quanto à privacidade e proteção de dados pessoais[7], na medida em que o ambiente inteligente pode reconfigurar a definição do espaço público-privado, permitindo a erosão da privacidade. Entrando num cenário de AmI parece implicar a perda de controlo sobre informações pessoais: "as ideias constitutivas de AmI, tais como "*pervasiveness*", a invisibilidade de sistemas de informação, a constante gravação automática de eventos etc. tornam altamente improvável que o usuário possa manter o domínio sobre como a informação é processada"(ROUVROY, 2008, p. 6).

O desenvolvimento de interfaces de percepção sensorial em sistemas de informação difusos e permeáveis ao contexto, exige "diretrizes de design específicas o suficiente para fornecer orientação significativa e flexíveis para ser usado em vários sistemas" (ROUVROY, 2008, p. 12), como o sistema de ODR. Procuraremos aferir se esta nova tendência de dispositivos específicos de tecnologia usável ou "*wearable*" transmite dados significativos e acionáveis quanto ao comportamento das partes. Neste artigo, descrevemos as principais preocupações que se suscitam num ambiente inteligente e conceituamo-lo no âmbito da mediação em linha. Analisamos a relevância, aplicabilidade e adequação do AmI dentro dos quadros legais da privacidade e proteção de dados (envolvendo os esclarecimentos e contribuições do Grupo de Trabalho do Artigo 29).

2 Os sistemas de mediação online em ambiente inteligente

Nesta secção, expomos as principais críticas dirigidas ao AmI e alocamo-las no quadrante do ODR. Propomo-nos a responder a algumas questões relativas à privacidade em computação ubíqua. Estará a tecnologia não só a limitar, mas também a alterar a privacidade, a identidade e a autonomia individual das partes envolvidas? Que mitos e preocupações podem ser desvendadas? Inferiremos possíveis respostas.

2.1 *Privacidade Online?*

As pessoas continuamente conectadas à rede ("*networked person*") (RODOTÀ, 2009, p.81) ou "*homo conectus"*, e em contexto de ambiente inteligente, encontram-se potencialmente sujeitas à monitorização de dados informacionais, pelo que se deparam mais permeáveis a violações da sua privacidade, o que nos conduz ao espectro de uma progressiva transformação das pessoas em "*pessoas eletrônicas*", objeto de constante monitorização. Nesta perspectiva, questiona-se se ainda é possível uma razoável expectativa de privacidade. Além disso, este aumento das possibilidades de monitorização fomenta ao progressivo

[7] Neste sentido, seguiremos a parametrização jurídica fornecida pela Diretiva 95/46/CE (UNIÓN EUROPEA, 1995).

esbatimento da distinção entre esfera pública e esfera privada e o perigo da "Vigilância de Dados" ou "Dataveillance" (DE HERT et al., 2009).

2.2 *Os dados pessoais e sensíveis recolhidos em ambiente inteligente*

A primeira questão que se coloca consiste no facto de a resolução de conflitos em linha, dotada de um ambiente inteligente, poder (ou não) cumprir com os requisitos da proteção de dados pessoais e sensíveis. Compulsados no atual quadro jurídico da UE, discernem-se categorias de dados. Dados pessoais são dados relativos a uma pessoa singular, identificada ou identificável, considerada titular dos dados. A Diretiva aplica um regime de proteção mais rigoroso para os dados sensíveis. A categoria de dados sensíveis, como retrata o artigo 8 º da Diretiva de Proteção de Dados da UE (Diretiva 95/46/CE, doravante denominada DPD) (UNIÓN EUROPEA, 1995), torna ilegal o processamento de dados pessoais reveladores de origem racial ou étnica, opiniões políticas, crenças religiosas ou filosóficas, filiação sindical, e dados relativos à saúde e à vida sexual. A Lei 67/98, em conformidade com a Diretiva Europeia, especificou esta proibição de modo a incluir no âmbito dos dados sensíveis, os dados relativos à vida privada, saúde, vida sexual e dados genéticos (PORTUGAL, 1998, art. 7º). Estas asserções revelam-se de especial acuidade, devido à potencial ameaça aos dados sensíveis extraídos num ambiente inteligente. De facto, os perfis construídos podem transmitir especificações sobre convicções filosóficas, status, personalidade. Enquanto que as imagens dos mediados provenientes de câmaras, previsivelmente fornecem informações sobre a sua vida privada, raça ou origem étnica e pistas visuais (como a forma de vestir, condição física, linguagem corporal e características pessoais, como a idade, sexo). O conjunto de dados informacionais coligidos em computação ubíqua, potencialmente poderá revestir natureza sensível (ou, como também se designa, "informação pessoal identificável"), sujeita a todo o tipo de interpretação (MOREIRA, 2010, p.471). Entende-se ainda que dentro desta noção de dados pessoais, deve incluir-se qualquer tipo de informação, de forma a que abarque as avaliações e apreciações sobre a parte envolvida, ou mesmo opiniões sobre o mesmo, escolhendo-se um critério subjetivo de dados, entendido como aquele que pode afetar direitos fundamentais.

Delimitado este quadro prescritivo e factual, sustentamos que o acesso aos dados pessoais relativos a uma disputa (de matriz consumerista) e armazenados na base de dados de ODR, só será concedido às entidades de resolução de conflitos a que os litígios tenham sido submetidos[8].

[8] Como dispõe o artigo 12º do Regulamento de ODR (UNIÓN EUROPEA, 2013).

As entidades de resolução de conflitos são consideradas responsáveis no que diz respeito às suas atividades de tratamento de dados exercidas ao abrigo deste Regulamento (UE) 524/2013 (UNIÓN EUROPEA, 2013), nos termos do artigo 2.º, alínea d), da DPD, e devem assegurar que essas atividades respeitem a legislação nacional adotada nos termos desta mesma Diretiva. Competirá à Comissão Europeia o tratamento dos dados pessoais dos utilizadores da plataforma de resolução de litígios apenas na medida em que tal seja necessário ao funcionamento e à manutenção da mesma, nos termos do art. 12.°, n.°2 do Regulamento de ODR.

2.3 *Identidade(s) diferente(s) ?*

Reside ainda o perigo/risco de que os dados coligidos, guardados, processados poderem ser transmitidos a terceiros (que poderão, por sua vez, ser humanos ou agentes eletrônicos). Estes agentes podem eventualmente incorporar e replicar elementos determinantes e constitutivos da identidade, atuando depois da mesma maneira como o correspondente sujeito agiria (NABETH, 2009, p.53). Competirá ressalvar que não são apenas os dados recolhidos que são importantes, mas o conhecimento gerado a partir dele. Vislumbra-se, pois, a oportunidade de cruzamento, relacionação e reelaboração de uma série de dados agregados que, aparentemente inócuos (a partir de imagens ou dados triviais e fugitivos, movimentos liberados voluntária ou involuntariamente pelos usuários), possam servir de conclusões e puzzles (MOREIRA, 2012) de natureza preditiva e errónea sobre o comportamento e facetas da vida das partes envolvidas. A questão do conhecimento gerado torna-se realmente pertinente, já que permite a transformação dos dados em conhecimento, atribuindo assim uma significação aos elementos recolhidos. Argumenta-se então que estes novos dispositivos de ambiente inteligente potencialmente reconfiguram a experiência humana e são susceptíveis de interferir com o processo através do qual as pessoas desenvolvem a sua própria personalidade (processo de "subjetivação") (ROUVROY, 2008, p. 4). Este novo ambiente tecnológico de AmI poderá, desta forma, contender com a clássica compleição de identidade que tende a correlacionar e vincular, de forma inequívoca, clássica e absoluta, uma identidade a uma determinada pessoa, como "um-para-um link" ("*a one-to-one link*") (OLIVIER, 2009, p.76). Pelo contrario, no quadrante da AmI, a ligação entre "uma pessoa-uma identidade", em princípio, já não se aplicará, pois que a identidade revelar-se-á cada vez mais fluída, indeterminada, variável e fragmentada. Neste segmento, a AmI poderá favorecer a tendência de multiplicação e polarização de várias e distintas identidades a partir de uma única (desta forma se designa a "era da identificação) (ANDRADE, 2011, p. 83).[9] Tal propensão, em particular, consistirá

[9] In the "Age of Identification", both public administrations and private entities, through automated profiling technologies, biometrics, monitoring and location technologies, will have at their disposal a set of advanced and

numa virtualização mais intensa e multiplicação de identidades distintas, com identidades virtuais e parciais a serem criadas para os mais diferentes fins e razões (tais como a segurança, possibilidade de negócio). No entanto, nesta incursão metodológica, visa-se capacitar as configurações de ODR com informações relevantes disponibilizadas durante o espectro, em detrimento de construções extensivas de perfis, recuperação de dados genéricos ou triviais, ou mesmo renúncia do controlo dos usuários sobre os seus dados.

2.4 *A tipificação de comportamentos inferidos em AmI e a autonomia das partes*

Correlativamente, esta monitorização pretende a construção e refinamento de perfis pessoais (*profiling*) a partir de dados comportamentais (in)voluntariamente cedidos pelas partes. Convocamos a seguinte dúvida: será que a construção de "perfis de utilizador" (secundados por movimentos, características de stress, de fadiga e estilos conflituais das partes) poderá interferir com a auto-percepção e autodeterminação das partes, a ponto de ser passível exaurir o sentido e conteúdo da autonomia individual (AGRE; ROTENBERG, 1998; CASTRO, 2005)? A produção e emulação de conhecimento inferido[10] relativo aos usuários poderá implicar a tipificação do comportamento das partes em categorias heterogéneas, de acordo com o estilo conflitual em questão. Relativamente à avaliação dos estilos conflituais das partes (através da análise do comportamento das mesmas enquanto interagem), tendemos a classificar as reações das partes de acordo, por exemplo, com a assertividade e cooperação das mesmas. A apreensão que urge excutir é *se* o comportamento de uma das partes (isto é, o seu comportamento como objeto de investigação, monitorizado, correlacionado com outras informações e, portanto, classificado), pode eventualmente afetar e restringir o próprio comportamento - entretanto classificado (e até aceite pelos padrões sociais), e se esse impacto sobre a parte em causa poderá, por sua vez, alterar esta classificação, reconfigurando a experiência humana (reconfiguração designada pela doutrina de "normalização de comportamento"[11], "*looping*

sophisticated instruments to identify, track and monitor their citizens or (potential) customers. Such new technological apparatus will render the various elements and aspects (indicia) of one's identity, protected under the right to personal identity (such as voice, physical appearance and psychological traits) more easily detected and, what is worst, more easily reproduced and replicated in the AmI scenario […]" (ANDRADE, 2011, p.83).

[10] Hildebrandt (2013) diferencia vários tipos de dados: i) dados concedidos a título voluntário, ii) dados observados (que frequentemente correspondem a dados comportamentais); e iii) dados inferidos, por exemplo, através de mineração de dados. Concretiza ainda a autora que os dados "voluntários" são definidos como explicita e conscientemente partilhados pelos seus titulares, como por exemplo, numa rede social ou em formulários contratuais. Reclama que a esta tipologia requer uma proteção jurídica também diferenciada.

[11] "This tech satisfy human needs and the human need is inscribed in the algorithmic "script" of the devices. Profiling techs are dynamic and adapt to human behavior, they operate within a certain formalized social ontology. They have a self-enforcing feedback effect on the behavior of users. According to the behavioral data, a user is matched to a certain profile. But the system will give feedback to the user and she will react conformingly. People will become segmented and stabilized. Is there a strategy of resistance to these normalizing process?" (DIJK, 2010, p.57-69).

effect"[12], de "*chilling effect*"(DE HERT et al., 2009) ou "*making up of people result*"[13]. Será que este "rastreio" e reconhecimento passivo de padrões comportamentais, legíveis e anotados por dispositivos, transformar-nos-á em "pontos de dados" ("*clusters" e "data-points"*) (HILDEBRANDT, 2013)?

No entanto, muitos dos nossos comportamentos (fadiga, stress, cooperação, passividade, entre outros) podem ser motivados por considerações totalmente alheias à própria natureza ou composição do litígio; desta indeterminação causal dos dados comportamentais, poderia percepcionar-se que: i) as categorizações-padrão dos comportamentos consubstanciariam inferências imprudentes; ii) requerer-se-ia um maior número de dados para consolidar padrões.

Ressalvamos no entanto que a matriz gestionária dos sistemas de AmI reside na capacidade de interação, adaptação e responsividade face aos seus usuários. Os dispositivos aditados ao contexto de ODR não são concebidos para criar ou modelar padrões de comportamento de uma das partes num determinado conflito, mas para observação de pistas contextuais com o objetivo de facilitar a comunicação entre as partes e o terceiro neutro, melhorar o desempenho deste facilitador em tempo real. Nesta intercorrência, avoca-se que a recondução do AmI à mediação online não subverterá a intencionalidade dos usuários, o seu poder de decisão, ou a sua autonomia. A conclusão de um acordo voluntário na mediação faculta aos participantes de ODR um controle sobre os resultados, aumentando as opções de resolução de conflitos, garantindo uma maior possibilidade do cumprimento do acordo encetado. A resolução de disputas em linha decorre do livre-arbítrio das partes e consiste num modelo de auto-composição. É baseado no princípio de que só as partes conduzem todo o processo para maximização dos seus interesses ("*interest-based approach*") e controlam os termos do processo e dos seus resultados (RULE, 2002) dentro de uma relação de confiança e dinâmica recíprocas.

Através de tecnologias de computação não invasivas, em ambiente inteligente, incorporadas num sistema de apoio à negociação, extraem-se funções potenciais que auxiliam proativamente os terceiros neutros durante o processo de decisional e na gestão da relação entre afeto e cognição *versus* negociação; a título de exemplo: *i)* detecta e avalia o contexto

[12] AmI visions rely on systems capable of 'learning' from occurring events and incrementally self-adjusting to respond optimally to human 'needs' whereas these "needs, are decreasingly defined by the concerned 'users' themselves, but increasingly defined according to the system's interpretations of whatever happens in the contexts, and of whatever users do or even, increasingly, of what their facial expressions and body motions are (ROUVROY, 2008).

[13] They are moving targets because our investigations interact with them, and change them. And since they are changed, they are not quite the same kind of people as before. The target has moved. I call this the 'looping effect'. Sometimes, our sciences create kinds of people that in a certain sense did not exist before. I call this 'making up people' (HACKING, 2007).

de interação dos usuários quanto ao processo de negociação e/ou mediação entre consumidor e agente económico (incluindo os níveis de escalabilidade dos comportamentos, as atitudes, os estilos pessoais de conflito, o estado emocional dos participantes (por exemplo, a passividade), ou os níveis de stress); *ii)* faculta informação ao terceiro neutro sobre como usar a emoção e o humor para favorecer a mediação; *iii)* habilita o terceiro neutro a interpretar as informações fornecidas e a estar ciente dos padrões e usos da comunicação online; *iv)* auxilia o terceiro a inteirar-se das suas próprias emoções e humor e dos seus efeitos sobre o processo de negociação e/ou mediação; *v)* consequentemente, sugere um comportamento estratégico e possível às partes. Sempre que o terceiro neutro percepciona uma mudança significativa na interação das partes, repensa as estratégias de comunicação definidas e reorienta o foco do processo de resolução de conflitos, a fim de manter as partes interessadas na sua resolução e encontrar formas mais adequadas de alcançar um resultado. Este processo continua até que seja possivelmente alcançado um acordo (CARNEIRO, 2012). Desta forma os facilitadores podem proporcionar um melhor apoio, permitindo que as partes prevejam as suas decisões e atuem cooperativamente. Contemplados com informações privilegiadas provenientes do AmI, o mediador pode orientar (FRIEDMAN; OLEKALNS; OH, 2007, p. 17) os disputantes sobre a melhor forma de apresentar os seus interesses e posicionar a sua "face"[14] ou "rosto". Em primeiro lugar, e independentemente da proposta substancial a apresentar por cada parte, devem evitar-se "ataques de face" (*face attacks*)[15]. Em segundo lugar, deve ter-se especial cuidado aos "*ataques de face-negativa*" que podem ser especialmente prejudiciais para qualquer esperança que recaia na reconstrução e prossecução do relacionamento comercial entre as partes. Neste sentido, consentaneamente referimos a importância de uma plausível comunicação enriquecida pelo *rapport* social e emocional que reforça a naturalidade dos diálogos das disputas em linha.

Da dinâmica proposta confia-se que os dados comportamentais colhidos figuram-se mais confiáveis e transparentes, dado o alinhamento desta tecnologia com os interesses dos intervenientes num processo de resolução de conflitos (CAMP; CONNELLY, 2007). Esta tramitação aproxima-se dos processos tradicionais de resolução de conflitos, nos quais as partes comunicam presencialmente e fazem uso do *feedback* percebido do contexto. Além disso, uma variedade de métodos de comunicação são utilizados durante o processo de

[14] "Face" ou **"**rosto" é o valor social positivo que uma parte efetivamente reivindica para si mesma em virtude da sua auto apresentação. Proteger a "face" é, de facto, central para as negociações e para o terceiro neutral que se sobrepõe ao conteúdo real do próprio acordo (FRIEDMAN; OLEKALNS; OH, 2007).

[15] O "ataque de face negativa" ocorre quando uma parte mina a vontade autónoma da outra parte e mostra falta de respeito, o que pode produzir "sentimentos de constrangimento e ansiedade / depressão. Os "*ataques de face positiva*" consistem em tentativas de desvalorizar a relação com a outra parte e estão "associados à percepção de menor e maior justiça encetada no relacionamento (FRIEDMAN; OLEKALNS; OH, 2007).

mediação e diferem de acordo com a (in)formalidade das sessões. A cadência de comunicação é, portanto, ajustada para atingir os melhores resultados na composição dialética. Prevê-se a coexistência de um equilíbrio performativo e fluído: o mediador e as partes podem fazer uso das sessões conjuntas, tais como, salas de mediação (*chat-rooms*) e *caucus* (BENFORD et al., 1993; KOHLER, 2003) para esclarecer e aprofundar imprecisões latentes que foram detectadas e possivelmente induzidas pela análise dos parâmetros fornecidos pelo ambiente inteligente. Esta personalização inerente à mediação em linha permite uma melhor ponderação e precisão quanto à autenticidade e fidedignidade dos dados compilados (assim, evitando o risco de valorar excessivamente algumas reações em detrimento de outras).

2.5 *Discriminação das partes*

Coloca-se ainda a questão se a construção automática de perfis (através da compilação de perfis detalhados dos usuários) discrimina as partes envolvidas (DIJK, 2010, p. 58). Efetivamente, o estabelecimento mecânico de perfis pode ser considerado como uma tecnologia discriminatória, uma vez que categoriza e diferencia pessoas (segmentação comportamental). Ressalvamos até uma possível margem de erro nesta categorização opaca e automática, e que poderá induzir a tipologias erróneas. Mas será uma discriminação justificável? A delimitação de perfis, neste caso em análise, não é uma questão de "*scoring*", nem uma questão de exclusão das partes da economia, de recursos ou oportunidades materiais ou informacionais (como por exemplo, delimitar o acesso ao crédito, "*scoring*" de um consumidor face ao seu risco segurável). Neste sentido, presumimos que se trata de uma discriminação justificada e tolerável uma vez que a informação qualificada e angariada através destes sistemas, não pretende excluir as partes da economia.

3 A privacidade e proteção de dados e a sua adequação face à resolução de litígios em linha e ambiente inteligente

A privacidade e proteção de dados encontra-se regulada na Diretiva de Proteção de Dados e nas Diretrizes da OCDE para Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais. Neste sentido, analisamos os principais princípios e comparamo-los com a textura inerente aos sistemas de ambiente inteligente, num cenário de ODR.

3.1 *Princípio da Limitação da Coleção de Dados e Consentimento*

O AmI, visto contingentemente, propõe uma agregação e análise algorítmica de dados sobre tudo e todos[16], ou "dataveillance" (CLARKE, 1988, p. 498), consubstanciando as partes como "super-processadores de informação" (ANDRADE; MONTELEONE, 2013, p. 119). Contudo, na acepção do ODR, importa a recolha de dados para cada processo de resolução de conflitos em linha em causa. Os dados pretendem-se operacionalizados num contexto delimitado de tempo e espaço: somente quando cada uma das partes acede ao sistema de ODR, os dispositivos são acionados para este efeito (cada sessão de mediação e durante cada processo de mediação) e, portanto, são desativados quando esse processo de mediação for concluído. Estes dispositivos detectáveis são relativamente fáceis de aplicar e constituem dispositivos pessoais e visíveis (CAS, 2011).

Para o processamento legítimo dos seus dados pessoais, é legalmente exigido que as partes envolvidas prestem o seu consentimento (artigos 2ºh) e 7º da Diretiva 95/46/CE (UNIÓN EUROPEA, 1995) e art. 7º nº 2 Lei 67/98 (PORTUGAL, 1998) através de manifestação de vontade concreta, livre e informada (PORTUGAL, 1998 art. 3º h)[17]. As partes devem subscrever um "termo de consentimento" que consiste num documento que reúne todos os princípios inerentes ao processo de mediação, estabelecendo-se como uma formalidade necessária para o início do processo. Deve, portanto, ser lido e assinado por todas as partes antes de o processo de mediação começar. Neste termo de consentimento, as partes são conhecedores da implementação das tecnologias de AmI. Isto implica que toda esta informação necessária deve ser dada no momento em que o consentimento é solicitado (artigo 10 º da Diretiva). Não obstante, quanto à validade do consentimento, os litigantes terão de fornecer o consentimento inequívoco (consentimento inteligível que especifique a finalidade exata do processamento), específico, expresso e informado (natureza granular do consentimento). Para significar este consentimento, a pessoa em causa deve preencher os formulários offline ou online, antes do início do processamento, que pode incluir uma assinatura manuscrita aposta ou através da utilização de assinaturas eletrônicas. Em relação

16 No entanto e em detrimento da minimização dos dados e da clássica proteção dos dados, equaciona-se o seu empoderamento ("data empowerment") no que toca ao acesso dos dados de todos por todos. Contrariamente à proteção de dados, que radica nos limites de partilha de informação, o "empoderamento dos dados" enfatiza precisamente a informação partilhada, possibilitando a todos a utilização de dados em "linked-data" relativos a vários contextos (dados informacionais relativos a saúde, cultura, economia, entre outros) (ANDRADE, 2011, p. 132) .

17 Devendo, no caso dos dados sensíveis, ser necessariamente um consentimento expresso. A exteriorização da vontade "[...] será livre se manifestada sem a intervenção de qualquer tipo de coação, direta ou indireta; será específica se concreta e precisa, afastando, deste modo, qualquer tipo de manifestação de vontade implícita. Será informada quando o titular dos dados esteja ao corrente dos efeitos que derivam da sua manifestação de vontade [...]" (CASTRO, 2005, p. 261-262).

aos dados sensíveis, como é o nosso caso, é amplamente admitido que o consentimento assinado é exigido *ad validitatem* (LE MÉTAYER; MONTELEONE, 2008, p. 8).

Em princípio, será suficiente ao controlador de dados obter o consentimento apenas uma vez, de acordo com o propósito específico de processamento de dados e de acordo com as expectativas razoáveis das partes (CASTRO, 2005, p. 207).

Cada parte poderá vetar o uso do sistema de monitorização (SOLOVE, 2004) e anular o consentimento anteriormente prestado a qualquer momento. O conhecimento adquirido durante o processo deverá ser destruído, uma vez concluso o litígio.

Neste sentido, os participantes de um sistema de ODR não se encontram dessensibilizados ou inconscientes aquando da prestação do seu consentimento (BROWNSWORD, 2009), nem consideramos a prestação do consentimento como um ato mecânico, automático ou perfunctório, ou a "rotinização do consentimento". Refere o Grupo de Trabalho do Artigo 29 (COMISIÓN EUROPEA, 2011)[18] que o consentimento obtido a partir da mera passividade ou silêncio tem uma ambiguidade intrínseca que não demonstra a vontade real da pessoa em causa. O consentimento deve ser expresso de forma positiva e não deve ser inferido a partir de configurações de privacidade.

3.2 *Princípio de qualidade dos dados*

Os dados pessoais devem ser relacionados com as finalidades da sua utilização e, na medida necessária, devem ser exatos, completos e permanecer atualizados. Este princípio comporta duas dimensões: i) a relevância dos dados para a prossecução da finalidade; e ii) a exatidão, integridade e atualidade dos dados.

A fim de obter dados mais precisos, deverá haver controlos regulares quanto ao processamento. Neste sentido, cada prestador de ODR deve ter um controlador no que diz respeito às suas atividades de processamento de dados, em conformidade com a alínea (d) do artigo 2.º da DPD e artigo 12.º, n.º4 do Regulamento de ODR. Neste sentido, o artigo 12.º n.º3 do Regulamento de ODR estabelece que os dados pessoais relacionados com a disputa são mantidos na base de dados ODR apenas durante o tempo necessário para alcançar os propósitos para os quais foram coligidos e são automaticamente eliminados, o mais tardar, 6 (seis) meses após a data de conclusão da disputa. Assim, evita-se a perpetuação do registo dos dados[19]. Os dados devem ser conservados apenas durante o

[18]O Grupo de Trabalho do Artigo 29 foi instituído pela Diretiva 95/46/CE (UNIÓN EUROPEA, 1995, art. 29). Trata-se de um órgão consultivo europeu independente em matéria de proteção dos dados e da privacidade. As suas atribuições estão descritas no art. 30.

[19] "[…] *perpetual appropriation of quite broad aspects of personal life*" (DE LA CUEVA, 1993, p. 69).

período necessário de acordo com as finalidades da recolha e do tratamento (PORTUGAL, 1998, art. 5.º nº 1e). Se os dados estão incorretos ou se são conservados para além do prazo limite, o titular tem o direito que os mesmos sejam eliminados ou, pelo menos, o acesso aos mesmos bloqueados. O que faz com que alguns autores expressamente refiram a necessidade de ser assegurada uma autodeterminação informativa ou até um direito à autodeterminação informacional (ROUVROY, 2009).

Finalmente, como corolário de um princípio de lealdade[20], os dados devem ser mantidos corretos, precisos e ser utilizados de acordo com a finalidade que foi invocada no momento da recolha, de um modo seguro e confidencial. E sempre que a finalidade que preside à utilização seja alterada, necessário se tornará um novo consentimento do titular (CASTRO, 2005, p. 207).

3.3 *Princípio de definição da finalidade ou da especificação do fim*

Este princípio transmite a ideia de que, pelo menos no momento da aquisição de dados, os fins são conhecidas e identificáveis. Na DPD (artigo 6.º b) é especificado que os dados pessoais devem ser recolhidos para finalidades determinadas, explícitas e legítimas. Os dados só podem ser usados de acordo com a finalidade que foi considerada no momento da sua recolha e esta finalidade deverá ser determinada, explícita, legítima. Os objetivos precisos e concretos do tratamento dos dados têm que ser indicados e os dados não podem ser utilizados contrariamente à referida finalidade. Mas a consideração deste princípio da finalidade não pode ser dissociado de outro requisito extremamente importante a ser observado no tratamento e processamento de dados: os dados recolhidos têm que ser apenas os necessários e adequados atendendo à referida finalidade e o tratamento e processamento não podem exceder aquilo que é realmente necessário para a prossecução das referidas finalidades. Ou seja, tem que ser respeitado o princípio da proporcionalidade, entre os dados que são colhidos e a finalidade que presidiu à sua recolha. Por outro lado, há que reconhecer que os critérios para apreciar a necessidade da recolha de dados hão de ser objetivos e de acordo com as finalidades expressas (CASTRO, 2005, p. 236).

Este princípio está correlacionado com o princípio da limitação da utilização que refere que os dados pessoais não devem ser divulgados, comunicados ou utilizados com finalidades

[20] Para que este direito seja considerado, necessária se torna a existência de um direito de acesso do titular aos dados (um direito de consulta que não necessita de ser justificado), mas sobretudo a existência de um direito de retificação e atualização dos dados e, com vista ao cumprimento de um verdadeiro controlo pelo titular, o direito à correção dos dados dentro de prazos determinados. Quer isto dizer que o titular dos dados deve ter o direito de verificar se os dados relativos à sua pessoa estão ou não corretos e, caso não estejam, deve ter o direito de retificação e atualização dos dados.

outras das que foram especificadas, salvo com o consentimento do sujeito dos dados, ou por força da lei.

A legitimidade da finalidade do processamento de dados e a sua compatibilidade com este princípio pode ser avaliada em relação à finalidade específica e pré-definida: para enriquecer e aumentar a eficiência do processo de comunicação na resolução de conflitos, com informações de contexto. Além disso, o conteúdo e o contexto em que este conhecimento é aplicado é claro no momento da coleta de dados.

O princípio da finalidade também inclui o princípio da transparência. O controlador deve cumprir com as exigências da DPD no tratamento de dados pessoais: os artigos 10.º e 11.º exigem que o controlador forneça ao titular dos dados: a) a identidade do controlador; b) os fins do tratamento a que os dados se destinam; c) outras informações, tais como os destinatários ou categorias de destinatários dos dados. A pessoa responsável pelo tratamento dos dados tem que estar claramente identificada, tendo que informar também claramente o titular dos dados sobre as finalidades e prazos para o tratamento e conservação dos dados ou sobre a sua comunicação a terceiros. Para além disto, este princípio da transparência claramente implica a existência de um direito à informação e de um direito de acesso aos dados (que tem que ser assegurado ao titular dos dados) e, sempre que tal seja legalmente exigido, o cumprimento de obrigações de registo, autorização, notificação à Comissão Nacional de Proteção de Dados.

4 Breves conclusões

Neste artigo, expomos que as críticas mais comuns dirigidas às ameaças à privacidade e proteção de dados em ambiente inteligente podem ser mitigadas quando visualizadas no contexto específico da resolução de litígios em linha.

Aferimos que a performatividade dos sistemas de inteligência ambiente aporta maior riqueza e apoio à resolução de litígios em linha que se pretende adaptada às estratégias em tempo real. Referimos que um ambiente inteligente é apto para suportar o ciclo de vida do conflito, e aporta conhecimento contextual importante, capaz de reagir a mudanças no contexto de interação, o que resulta numa abordagem de resolução de controvérsias capaz de perceber as partes, alterar estratégias de atuação e, consequentemente, alcançar melhores resultados. No entanto, esta compleição obriga-nos a repensar questões relacionadas com a identidade e autodeterminação da pessoa humana, a privacidade, a proteção de dados, a transparência dos sistemas, o consentimento das partes e a finalidade da recolha de dados, questões que analisamos neste artigo. Na apreciação dos requisitos atinentes à privacidade e

proteção de dados que são pertinentes no contexto de computação ubíqua, consideramos necessário espaços de normatividade ou "pluralismo normativo" (WINN, 2009), incluindo o direito, a tecnologia, as partes interessadas no domínio das TIC e a sociedade terão de ser proativos de forma a que a legislação relativa ao ODR e à privacidade e proteção de dados possa evoluir para acomodar os novos desafios colocados pela AmI numa perspectiva comunicativa e evolucionista e que se aperfeiçoem as tecnologias indutoras de transparência[21] (TETS). A necessária conceituação entre o AmI (um sistemas orientados para as partes que utilizam informação sensível sobre o utilizador) e a proteção dos dados pessoais terá de ser ponderada. O que se torna vital é a proteção do utilizador e dos dados que fluem no sistema, de modo a que o utilizador possa beneficiar dos serviços disponibilizados sem deixar de estar, ao mesmo tempo, legalmente protegido.

No presente estádio da pesquisa (aliando as sinergias do AmI ao ODR), é complicado oferecer algo mais do que reflexões modestas tendo em vista a sua inclusão na revisão da legislação atinente à Proposta de Regulamento Geral sobre a Proteção de Dados (COMISIÓN EUROPEA, 2012). A configuração entre AmI e ODR requer ainda maior pesquisa para a sua consolidação. No entanto, este advento é uma linha de pesquisa promissora para o futuro do ODR.

5 Agradecimentos

O trabalho apresentado neste artigo é suportado pelo projeto CROWDSOURCING: Instrumentos Semânticos Para el Desarrollo de la Participacion y la Mediacion Online Referência: DER2012-39492-C02-01 - Ministerio de Economía y Competitividad. DGICYT.Subdirección General de Proyectos de Investigación - Espannha.

6 Referências

AGRE, P. E.; ROTENBERG, M. (Eds.). **Technology and Privacy**. The New Landscape. Massachusetts: MIT Press, 1998.

ANDRADE, F. Comunicações Electrónicas e Direitos Humanos: o perigo do "homo conectus". In: MONTE, M. F.; BRANDÃO, P. T. (Coords.). **Direitos Humanos e sua efetivação na era da Transnacionalidade**: debate luso-brasileiro. Curitiba: Juruá Editora, 2012. p. 207-226

ANDRADE, N. N. G. **Right to Personal Identity**: The Challenges of Ambient Intelligence and the Need for a New Legal Conceptualization. In: GUTWIRTH, S. et al (Eds.). **Computers, Privacy and Data Protection**: an element of choice. Dordrecht, Heidelber, London, New York: Springer, 2011. p. 65-97.

[21] Ou "*Transparency Enhancing Technologies*".

_____; MONTELEONE, S. Digital Natives and the Metamorphosis of the European Information Society. The Emerging Behavioral Trends Regarding Privacy and Their Legal Implications. In: GUTWIRTH, S. et al. (Eds.). **European Data Protection**: Coming of Age. Dordrecht, Heidelberg, New York, London: Springer, 2013. p. 119-144.

BENFORD, S. et al. From Rooms to Cyberspace: Models of Interaction in Large Virtual Computer Spaces. **Interacting with Computers**, v. 5, n. 2, p. 217-237, june/1993.

BROEKENS, J.; JONKER, C. M.; MEYER, J. C. Affective Negotiation Support Systems. **Journal of Ambient Intelligence and Smart Environments**, v. 2, n. 2, p. 121-144, apr./2010.

BROWNSWORD, R. Consent in Data Protection Law: Privacy, Fair Processing, and Confidentiality. In: GUTWIRTH, S. et al. (Eds.). **Reinventing Data Protection?** [S.l.]: Springer, 2009. p. 83-110.

CAMP, J.; CONNELLY, K. Beyond Consent: Privacy in Ubicomp. In: ACQUISTI, A. et al. (Eds.). **Digital Privacy:** Theory, Technologies and Practices. Boca Raton, Auerbach Publications, 2007. p. 1-17.

CARNEIRO, D. et al. Developing dynamic conflict resolution models based on the interpretation of personal conflict styles. In: ANTUNES, L.; PINTO, H. S. (Eds.). **Progress in Artificial Intelligence**. Lecture Notes in Computer Science, v. 7026. Berlin, Heidelberg: Springer, 2011. p 44-58.

CARNEIRO D. et al. Context-aware Environments for Online Dispute Resolution. In: INTERNATIONAL ANNUAL MEETING OF THE GROUP DECISION AND NEGOTIATION CONFERENCE, 12., 2012, Recife. **Proceedings**… Recife: Ed. Universitária da UFPE, 2012. p. 196-216

CASANOVAS, P.; POBLET, M.; LÓPEZ-COBO, J. M. Relational Justice: Mediation and ODR through the World Wide Web. In: STEINER, F. (Ed.) **Archivfürrechts-und sozialphilosophie**. Stuttgart: ARSP, 2011. p. 319-336.

CAS, J. Ubiquitous Computing, Privacy and Data Protection: Options and Limitations to Reconcile the Unprecedented Contradictions. In: GUTWIRTH, S. et al (Eds.). **Computers, Privacy and Data Protection**: an element of choice. Dordrecht, Heidelberg, London, New York: Springer, 2011. p. 139-169.

CASTRO, C. S. **Direito da Informática, privacidade e dados pessoais**. Coimbra: Almedina, 2005.

CLARKE, R. Information Technology and Dataveillance. **Communications of the ACM**, v. 31, n. 5, p. 498-512, 1988.

COMISIÓN EUROPEA. **Parecer 15/2011 sobre a definição de consentimento**. Grupo de Trabalho de Protecção de dados do Artigo 29.º 01197/11/PT WP187. Bruxelas: [s.n.], 2011. Disponível em: <http://www.gpdp.gov.mo/uploadfile/others/wp187_pt.pdf>. Acesso em: 6 maio 2014:

_____. **Proposta de Regulamento do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (regulamento geral sobre a proteção de dados)**. COM(2012) 11 final. Bruxelas, [s.n.], 2012.

DE HERT, P. et al. Legal Safeguards for Privacy and Data Protection in Ambient Intelligence. **Personal and Ubiquitous Computing**, v. 13, n. 6, p. 435-444, aug./2009.

DE LA CUEVA, P. L. M. Informática e protección de datos personales. **Cuadernos y Debates**, Madrid, n. 43, 1993.

DIJK, N. V, Property, privacy and personhood in a world of ambient intelligence. **Ethics and Information Technology**, v. 12, n. 1, p. 57-69, mar./2010.

FRIEDEWALD, M. et al. The Brave New World of Ambient Intelligence: An Analysis of Scenarios regarding Security, Security and Privacy Issues. In: CLARK, J. A. et al. (Eds.). **Security in Pervasive Computing.** Lecture Notes in Computer Science Series, v. 3934. New York: Springer, 2006. p. 119-133.

FRIEDMAN, R.; OLEKALNS, M.; OH, S. H. Choosing Your Words Carefully: Managing 'Face' During On-Line Dispute Resolution. In: ANNUAL CONFERENCE OF THE IACM, 20., 2007, Budapest. **Proceedings**… Budapest: IACM, 2007. p. 4-33. Disponível em: <http://ssrn.com/abstract=1111637>. Acesso em 6 maio 2014.

HACKING, I. Making Up People. **London Review of Books**, v. 26, n. 16, p. 7-11, aug./2007.

HAMMOND, A. G. How do you write "yes"? A study on the effectiveness of online dispute resolution. **Conflict Resolution Quarterly**, v. 20, n. 3, p. 261-286, Spring/2003.

HILDEBRANDT, M. Slaves to Big Data. Or Are We? **IDP**: Revista de Internet Derecho y Politica, Barcelona, v. 16, jun./2013. (*forthcoming*). Disponível em: <http://works.bepress.com/mireille_hildebrandt/>. Acesso em 8 jun. 2014.

KOHLER, G. K. La resolución de los litigios en línea – perspectivas y retos del contencioso internacional contemporáneo. **Revista Latino-Americana de Mediación y Arbitraje**, v. 3, n. 4, 2003.

LE MÉTAYER, D.; MONTELEONE, S. Computer Assisted Consent for Personal Data Processing. In: CONFERENCE ON LEGAL SECURITY AND PRIVACY ISSUES IN IT (LSPI'2008). 3., 2008, Prague. **Proceedings**.... Prague: IAITL, 2008, p. 29-41. Disponível em: <http://pop-art.inrialpes.fr/~lemetayer/lspi2008.pdf>. Acesso em: 6 maio 2014.

MOREIRA, T. C. **A Privacidade dos Trabalhadores e as Novas Tecnologias de Informação e Comunicação**: contributo para um estudo dos limites do poder de controlo eletrónico do empregador. Coimbra: Almedina, 2010.

_____. Novas Tecnologias: um admirável mundo novo do trabalho? **Revista de Direitos e Garantias Fundamentais**, Vitória, n. 11, p. 15-52, jan./jun. 2012.

NABETH, T. Identity of Identity. In: RANNENBERG, K.; ROYER, D.; DEUKER, André (Eds.). **The Future of Identity in the Information Society**: Challenges and Opportunities. Berlin, London: Springer, 2009. p. 19-69

OLIVIER, D. et al. Virtual Persons and Identities. In: RANNENBERG, K.; ROYER, D; DEUKER, A. (Eds.). **The Future of Identity in the Information Society**: Challenges and Opportunities. Berlin, London: Springer, 2009.

PEREIRA, M. Opinião: Como seria o mundo se os objetos também comunicassem? **TEK**, 31 jan 2014. Disponível em: <http://tek.sapo.pt/opiniao/opiniao_como_seria_o_mundo_se_os_objetos_tamb_1363005.html>. Acesso em: 05 fev. 2014.

POBLET, M. et al. Tecnologías para la mediación en línea, estado del arte, usos y propuestas. In: CASANOVAS, P.; MAGRE, J.; LAUROBA, M. E. (Eds). **Libro Blanco de la mediación en Catalunya**. Barcelona: Huygens Editorial, 2011. p. 943-1008.

POBLET, M.; CASANOVAS, P. Emotions in ODR. **International Review on Law, Computers, and Technology**, v. 21, n. 2, p. 145-156, 2007.

PORTUGAL. Lei n° 67/98 de 26 de outubro. Lei da protecção de dados pessoais. **Diário da República**, Lisboa, 26 out. 1998. I Série A, n. 247, p. 5536- 5546.

ROUVROY, A. Privacy, Data Protection and the Unprecedented Challenges of Ambient Intelligence. **Studies in Ethics, Law and Technology**, v. 2, n. 1, article 3, 2008. Disponível em: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1013984>. Acesso em: 6 maio 2014.

RULE, C. **Online Dispute Resolution for Businesses**. B2B, E-Commerce, Consumer, Employment, Insurance, and Other Commercial Conflicts. San Francisco: Jossey-Bass, 2002.

RODOTÀ, S. Data Protection as a Fundamental Right. In: GUTWIRTH, S. et al. (Eds.). **Reinventing Data Protection?** Dordrecht, London: Springer, 2009. p. 77-82.

SOLOVE, D. J. **The Digital Person: Technology and Privacy in the Information Age**. New York University Press, 2004.

UNIÓN EUROPEA. Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. **Diario Oficial de las Comunidades Europeas**, Luxembourg, 23 nov. 1995. L. 281/31, p. 31–50.

_____. Reglamento (UE) 524/2013, del Parlamento Europeo y del Consejo de 21 de mayo de 2013 sobre resolución de litigios en línea en materia de consumo y por el que se modifica el Reglamento (CE) no 2006/2004 y la Directiva 2009/22/CE (Reglamento sobre ODR de consumo). **DOUE**, Unión Europea, Estrasburgo, 18 jun. 2013. L 165, p. 1-12.

WAHAB, M. S. A. Does Technology Emasculate Trust? Confidentiality and Security Concerns in Online Arbitration. In: ICC. **Using Technology to Resolve Business Disputes**. Special Supplement – ICC International Court of Arbitration Buletin, n. 667. [S.l.]: ICC, 2004. p.43-52.

WEYRICH, C. **Orientations for Workprogramme 2000 and Beyond**. [S.l.]: European Commision ISTAG, 1999.

WINN, J. K. Technical Standards as Data Protection Regulation. In: GUTWIRTH, S. et al. (Eds.). **Reinventing Data Protection?** [S.l.]: Springer, 2009. p. 191-206.