Increasing media richness in Online Dispute Resolution and the need for personal data protection

Cristiana SANTOS[a]
[a] *Phd candidate of the Joint International Doctoral Degree in Law, Science and Technology and the Universitat Autònoma de Barcelona, Institute of Law and Technology, Spain*

Abstract. This contribution introduces a new approach to online dispute resolution (ODR) and provides a portrayal of the performativity that Ambient Intelligence systems seem to convey to ODR: substantial enrichness and levels of support to the decision-making process with the provision of meaningful context information. We will portray the main issues and concerns addressed to Ambient Intelligence and we conceptualize them in the prism of online mediation. We will detail an analytical approach towards deconstructing the AmI scenario envisioned in online mediation context. We will frame privacy and data protection in the prospect of the emerging challenges raised by the development of information and communication technologies and through the filter of the ODR Regulation.

Keywords. ODR, Ambient Intelligence, Media Richness, Context-awareness, Data Protection, Privacy, Regulation

Introduction

Leading research has shown that mediation[1], as a consensual method of dispute resolution, appears to be particularly suitable to manage and solve consumer disputes [1] and has become a legal functionality [2] incorporated in the daily legal routine. According to the recent conclusions and current applications in the domain of Online Dispute Resolution[2] [3], emotions emerging in online interactions can be identified as "social functions", "contextual cues" or "indexes" in virtual environments (such as

[1] Mediation means a structured process, however named or referred to, whereby two or more parties, on a voluntary basis, try to reach an agreement on the settlement of their dispute with the assistance of a mediator. This process may be initiated by the parties or suggested or ordered by a court or prescribed by the law of a Member State, as stated in Article 3 (a) of the Directive 2008/52/EC, of the European Parliament and of the Council of 21 May 2008 on certain aspects of mediation in civil and commercial matters (OJ L136/3).

[2] Regulation n. º 524/2013 of the European Parliament and of the Council on online dispute resolution for consumer disputes (Regulation on consumer ODR), hereinafter termed simply as ODR. We consider ODR as a communicative process involving the parties engaged in an interactive decision-making task, as a mean for consumer redress. Therefore, "emotions" are an essential component in any online dispute process. Emotions have interpersonal effects on mediators that monitor the parties' emotions and use them to estimate their limits, to adjust their demands and anticipate possible obstacles to conflict resolution, therefore, shaping individual's attitudes towards the communicative and informational flow.

facial gestures, voice inflection, intonation, etc). These conclusions propose that online communication culture has parameterized its own "paralinguistic cues to express emotions (i.e. through special characters, emotions, use of capital letters, etc)." Recent findings on ODR embrace that ODR is not "emotionally limited" and may moderate major concerns about ODR as an impersonal environment, where emotions cannot be used as contextual or interactive cues. Empirical studies conclude that ODR "allows disputants to be more thoughtful in their submissions, to evaluate their emotions and express them rationally and engage at their own pace" [3]. Moreover, research has shown that pre-communication reframing and caucusing with the participants can sustain a balanced communication within a given dispute. By contrast, the most frequently concerns about ODR skeptics[3] consists that online processes cannot match the richness of the face-to-face interactions and commentators often define that parties communicating screen-to-screen are likely to experience low levels of interpersonal trust, and raise concerns about confidentiality, security, identity and higher rates of deterioration than those engaged in face-to-face interaction [5]. Cognitively, we posit that online dispute resolution "situates and intensifies the strength and the content of the communication flow"[6].

The performativity of AmI systems[4] seems to convey substantial enrichment and higher levels of support (as a serviceable tool) to online dispute resolution [7]. Thus, ODR services and technology must be constructed in such a way that their interveners will trust them as an efficient and effective way of managing their disputes [8].

Nevertheless, the fact that this environment surrounds the users and constantly acquires information about them and their context of interaction, by means of regular devices with computational power (e.g., touch screens, video cameras, accelerometers, PDAs), brings along legal requirements concerning the consent of the users and the finalities of the use of the collected data that we propose to analyze. To acquire maximum advantage from ambient intelligence, it becomes compulsory to forecast and respond to possible drawbacks and threats emerging from the new technologies[5], in

[3] Online interactions, when compared to face-to-face communication, are seen as impersonal, lacking human interaction and unable to express non-verbal cues (such as the variable tone, pitch and volume).

[4] The term Ambient Intelligence (AmI) was coined by Emile Aarts and taken up by the Advisory Group to the European Community's Information Society Technology Program (ISTAG) as the convergence of ubiquitous computing, ubiquitous communication and interfaces adapting to the user. The concept of AmI depicts a vision of the future information society, where the emphasis is on greater user-friendliness, more efficient services support, user empowerment, and support for human interactions. As an illustrative instance, during 2008, the number of things connected to the internet exceeded the number of people on earth and "these things are not just smartphones and tablets. Increasingly, the objects in our lives can now talk to us and this isn't just about health, it's also about manufacturing, the auto industry, business, government, science and everyday life. In the not too distant future, everybody, everything and every object will become a communication platform. These things are tracking our lives, giving us data about things we've never measured before. In 2014, there will be 400 million of these devices (...)", Rachel Kalmar, Data Scientist at Misfit Wearables, http://www.slideshare.net/kalmar1. As a new trend and wave of the nascent marketable technologies, the future of networked computing is called "Body Computing" and regards the wireless and mobile devices that are implanted in human bodies or wearable, both aesthetically and practically, that will one day control the future of health, lifestyle management and communication, among other things, in http://project10x.com/.

[5] Recent prototypes try to apply emotions in computer-mediated-communication, such as linguistic models to tag chat conversation with emotion tags; or even through information visualization interfaces, that enables a user to input a real-time continuous flow of their predominant emotion, by using a color spectrum which provides an insight into when, how and with what degree of certainty opinions were developed and changed over time.

order to devise and furnish appropriate safeguards regarding privacy and data protection.

The foreseen concerns unfold towards the "*homo-conectus*"[9] as the technology develops. In fact, the realm of AmI is reconfiguring and blurring the definition of the private-public space continuum, allowing the erosion of privacy. Entering in an AmI scenario appears to entail the loss of control over personal information: "the constitutive ideas of AmI, such as pervasiveness, invisibility of information systems, constant and automatic recording of events etc. render highly implausible that the user will retain control over what and how information is processed"[10]. The development of value-sensitive perceptual interfaces in pervasive and context-aware information systems, requires "design guidelines that are both specific enough to provide meaningful direction and that are sufficiently flexible to be used across systems"[10] (as the ODR system). We will seek if these new trend of specific wearable technology devices convey the meaningful and actionable data about the parties behavior within the data ecosystem.

In this line, ODR studies [11] assert that IT is not fully employed within the current ODR systems [6] [12, 6]. Conversely, the incorporation of new technologies with high penetration in different world areas may facilitate the development of ODR services: mobile penetration has grown dramatically over the past decade, and it seems that services attached to mobile devices will increase accordingly [13]. In fact, mobile artifacts are portable, durable, basic and relatively low-cost, whereas they employ easy-to-use technology and have far-reaching functionalities [14]. These characteristics might suggest that mobile devices (which incorporate sensors) may be particularly appropriate for empowering consumers in the ODR process within an AmI scenario. Moreover, empirical evidence concluded that synchronous online communication (such as chats or video-conference that are proposed in this paper) had a much higher rate of win-win solutions compared to delayed communication (asynchronous tools) [3].

In this paper, we introduce a new approach to online dispute resolution. We will describe the main issues and concerns addressed to AmI and we conceptualize them in the prism of online mediation. We will detail an analytical approach towards deconstructing AmI scenario envisioned in online mediation context. Consequently, we will frame privacy and data protection *i)* in the prospect of the emerging challenges raised by the development of information and communication technologies (on the threshold of an "ambient intelligence era"); and *ii)* through the filter of the ODR Regulation. We will assess the relevance, applicability and adequacy of the European privacy and data protection legal frameworks (encompassing the European Union Article 29 Working Party contributions and clarifications) towards these unprecedented challenges.

[6] In order to have a more forthcoming and practical insight, we quote the author excerpt "(...)The Wikipedia dispute resolution system is perhaps one of the few hallmarks of ODR 2.0: processes are highly flexible, interactive, and collaborative. But, how may other ODR initiatives benefit from both the trends and opportunities of Web 2.0? Colin Rule predicted in 2006 that ODR would be one of the biggest beneficiaries of these new technologies, because they are squarely aimed at ODR's core functionality areas: communication, collaboration, and interactivity. However, he also warned that too many ODR providers rely on outdated platforms and technology because they are reluctant to make the investments in time and resources needed to bring their platforms up to Web 2.0 standards. Colin Rule also asserts that costs have an impact on not only access but also to perceptions of distributive justice. If ODR is less expensive than other alternatives, it enhances access. Outside big marketplaces, however, there are few business models for sustainable ODR systems" [6, 12].

1. Are online mediation AmI systems compatible with privacy?

In this section we will try to expose some of the critics addressed to AmI and allocate them in the ODR framework. We will also try to respond to some primary questions on privacy and ubiquitous computing: which differences will an ubiquitous computing environment shift in our concrete lives? Is technology not only limiting, but also altering privacy? What myths and grounded concerns can be unraveled? Hereby we will try to evaluate possible answers.

Current EU legal framework differentiates the categories of data and applies a stricter protection regime towards the sensitive data. The category of sensitive data, as depicted in article 8.º of the EU Data Protection Directive (Directive 95/46/EC - hereinafter termed simply "the Directive"), makes it illegal to process personal data[7] revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health or sex life. This is relevant particularly due to the potential threat of AmI applications to sensitive data. Images collected from the parties predictably provide information about their private life, their racial or ethnic origin; profiling parties on the basis of the very nature of the conflict (such as a consumer conflict) may transmit specifications about those persons' philosophical beliefs and status, while videos disclose visual cues (like dress, physical condition or body language and personal characteristics, as age, sex). The multitude of linking data from different sensors implies that data collected by the ubiquitous computing, are, in principle, personal data[8] or as it is also defined, "personally–identifiable information"[15].

The online mediation approach tries, in principle, to comply with data protection requirements. Processing of personal data is enclosed in Article 12 (1) of the Regulation on consumer ODR that says that access to information, including personal data, related to a dispute and stored in the ODR database shall be granted only to the ADR and ODR entities to which the dispute was transmitted. Also, all the sensitiveness of the personal data processing is submerged to the confidentiality principle settled in Article 7 of the ADR Directive (Directive 2013/11/EU): the third neutral can not reveal data conveyed during the mediation and that the parties did not authorize to disclose. [9]

It is argued that this new tools that "potentially reconfigure human experience, may also interfere with the process through which individuals come to build their own personality (process of "subjectivation") [10] and individual autonomy[10] [16 at 3] (as the "freedom from unreasonable constraints on the construction of one's own identity"). Reconducting AmI within the online mediation environment may encompass users´ intentionality, decisional power and a sense of control. The completion of a voluntary agreement in mediation, gives ODR participants a greater control over the results and

[7] The Data Protection Directive applies to the processing of "personal data", defined as any information relating to an identified or identifiable natural person ("data subject"). Article 2 of the Directive defines an identifiable person as one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his psychic, psychological, mental, economic, cultural or social identity.

[8] Article 29 Data Protection Working Party. Opinion 4/2007 on the Concept of Personal Data.

[9] Within this purpose, the Commission shall take the appropriate technical and organizational measures to ensure the security of information processed under the ODR Regulation, including appropriate data access control, a security plan and a security incident management, Article 12 (2).

[10] "(...) control over personal information is control over an aspect of the identity one projects to the world and the right to privacy is the freedom from unreasonable constraints on the construction of one's own identity [16].

control over their personal information, increasing the options for resolving conflicts without the limitations imposed by law and ensuring greater possibility of its fulfillment. ODR mediation system stems on the free-will of the parties and consists in a self-composed model. The processing of conflict resolution is based on the principle that only the parties will conduct all the process and will operate in the realm of maximization of their interests (in an interest-based approach) and are the ones who control the terms of the process and its results [17] within an inter-party trust dynamic.

The information systems involved in AmI visions intends to observe the unique complexity of each individual human being, which makes possible to emulate and produce knowledge about their users (by profiling). But in regarding to the acquired knowledge, it might typify individuals in a variety of heterogeneous categories, according to their conflict resolution style [10]. Regarding the assessment of personal conflict resolution styles (by analyzing the behavior of the disputant parties whilst they are interacting), we tend to classify their response according to the individual's assertiveness and cooperativeness. The apprehension here is to identify *if* the behavior [18] of a targeted party (its traces taken as object of scientific inquiry, monitorized, characterized, matched with other information and therefore classified), may possibly *affect* and constrain the people's classified behavior and actions (up to the standards accepted by the majority), and the effects on the people, in turn, change the classifications", and if it may possibly reconfigure human experience, revealing the "looping effect"[11] [10], or the "chilling" effect" [19] and the "making up of people" [12] [20] result. AmI systems vocation is described as "human centered", reactive to the individual's choices and needs and oriented towards empowering their users (therefore evades from the "Kafka metaphor"[13]) [21]. The engines involved in an AmI scenario provide real assets but aren't envisioned nor conceived for "making up" the intervenors of a mediation process, nor to create or mold behavioral patterns of either party in a given conflict, but for observation of contextual meaning in order to help to facilitate communication for the conflict manager, advise upon potential solutions and enhance the mediator's performance to obtain a better framed and realistic decision in real-time.

Another alleged concern relies in the possibility that the deployment of AmI technologies might *construct* or *produce* meaningful knowledge, even from trivial and fugitive image, sound or movement captured voluntarily or involuntarily released by the users, and within this conceptualization, would epitomize the "frame of the user's environment in ways that would impact and interfere on their self-perception (...), and their capacity for self-determination[14] [22]. In this line of research we aim to empower ODR settings with estimated information about the levels of stress of the parties *rather than* extensive profiling, retrieving generic or trivial data, or even waiving the users' control upon their data. We acknowledge that the ability of a mediator to form rapport

[11] "(...) 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"[10, at 13].

[12] (...) "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'"[20].

[13] The author explains the "Kafka metaphor" through the idea of the helplessness and the vulnerability that individual's face regarding the powerful bureaucracies that handle their personal data.

[14] In article 35. º of the Portuguese Constitution is depicted the right to informational self-determination.

with parties has been found to be the most important skill a mediator can possess [23] in order to accomplish an integrative, win-win outcome. It has been observed that the social rapport and the physical and emotional cues, on the bases of correlated data, will enhance the naturalness of the emerging negotiation dialogues and thus increasing the richness of the communication medium. Whenever the mediator notices a significant change in the interaction, it induces to the rethinking of the strategies defined and to the re-orientation of the focus of the conflict resolution process in order to keep the parties interested in its resolution and to find more suitable ways of achieving an outcome. Specifically, whenever the mediator feels that it is necessary, he may choose to adapt these strategies. In order to decide when and how to perform this adaptation, the mediator interprets the information provided by an intelligent environment about the context of interaction, including the levels of escalation, the attitudes, the personal conflict styles, the emotional state (e.g. passive or emotionless behavior) or the levels of stress. This process goes on until a party leaves the process or a successful agreement is reached [41].

With this high level of "informational, emotional, relational privacy" [25] data, mediators can provide better support, enabling parties foreseeing their decisions and subjects can be more cooperative, which can result in more reliable data. In this way we argue that privacy can enhance data reliability [26] in AmI by alignining technology with the parties' interests. This endeavor approaches to traditional processes in which people communicate face-to-face and make use of the perceived feedback of the context. As soon as the relevant information is made available during the negotiating spectrum, the content of the agreement will be more consensual ("interested-based approach"), reducing the information gap that may exist and its "negative expected value"[27].

Moreover, a variety of communication methods are currently used during the mediation process and differ according to the (in)formality of the sessions, the constancy of the state of mind of the parties and the balance of power. The cadence of communication is thus adjusted to achieve the best results in the dialectic composition. It is envisaged the coexistence of a performative and fluid balance: the mediator and the parties can make use of the joint sessions, such as mediation rooms [28], online *caucus* [29] and follow-up interface (even to clarify and deepen latent inaccuracies that were detected and plausibly induced by the analysis of these parameters provided by intelligent artifacts). This personalization/customization inherent to online mediation paradigm -*mediate-centered* approach -, allows for better weighting, pondering and accuracy as to the authenticity and trustworthiness of the compiled data (and thus avoiding risks of overly weighting some reactions over others).

The applied apparatus (tactile screen and cameras) simplify users' experience so that the parties can feel they are in control of their data and that this linking and merging of data is managed in an accountable way. If users are not willing to be involved in the active protection and management of their digital assets, the trusted third party (mediator) could do this on their behalf and could provide them with easy-to-use tools to monitor and keep the situation under control.

We are already living in a world of "ubiquitous data availability" and we need pervasive privacy preserving solutions. As ambient intelligence challenges existing legal protection of privacy, conceiving and designing privacy friendly legal safeguards systems has become a priority [30], as enclosed by the "Security Safeguards Principle" that states that "personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or

disclosure of data"(Paragraph 11, OECD Guidelines). Regarding implementations of new and mindful security proposals, we are thus overcoming the "titanic phenomenon"[31][15] and anticipating the consequences of what can go wrong before embracing a new technology. The existing legal framework contains some important safeguards for privacy and data protection: "by default, privacy law protects the *opacity* of the individual, while data protection, also by default, calls for *transparency* of the processor of personal data"[16][19]. "However, we envisage a new paradigm where the default position will be the use of transparency tools. If the goal of regulation is to control or channel the exercise of power rather than to restrict it, then transparency tools seem more appropriate than opacity tools. In such situations, the collection and processing of data would thus be allowed, but made controllable and controlled" [19]. Therefore, transparency tools could offer a solution to some of the legal problems raised by AmI. Also, a global technical standard of data protection is needed, to support data protection laws [31].

2. Relevance, applicability and adequacy of the European privacy and data protection legal frameworks to the challenges in AmI

The instantiation of privacy and data protection is based in the European Data Protection Directive and in the important provisions listed in the OECD Privacy Guidelines that compound the classical "Fair Information Practice" principles of data protection law. In this regard and for our purposes, we will proceed with its essential legal features and we will compare with some inherent textures of computing systems, although mitigated with ODR principles. We will only give particular attention to those that exert influence and intersect to the configuration of ODR in an AmI environment.

2.1. Collection Limitation Principle and Consent (Article 6 (c) of the Data Protection Directive)

The envisioned non-invasive (and transparent to the user) approach appears to comply with the above principle. AmI, viewed contingently, purports the massive collection, aggregation and algorithmic analysis of data on everyone and everything ("dataveillance" [17] [19] or "panoptic society").[18] But the ensuing analysis of this data, in the ODR perception, has to be enforced by the data minimization principle (that allows collecting as little data as necessary for a given purpose) and shaped by the principle of

[15] The impressive term coined by Solove consists in the premise that due to the rapid pace of innovation, new mindful and technological artifacts should be first pondered and evaluated in practical terms before its deployment [31, at 199].

[16] As stated in Article 12 (4) of the ODR Regulation, each ODR advisor shall be regarded as a controller with respect to its data processing activities under this Regulation, in accordance with point (d) of Article 2 of Directive 95/46/EC, and shall ensure that those activities comply with national legislation adopted pursuant to Directive 95/46/EC.

[17] "(...) The lifeblood of AmI is, the massive collection, aggregation and algorithmic analysis of data on everyone and everything. Dataveillance brings about the second big challenge for privacy protection: the blurring of boundaries between what is private and what is public. In an AmI environment, different spaces and activities overlap. How (or even if) we can distinguish between what is private and what is not, and how privacy can be protected when its boundaries are increasingly blurred?" [19, at 2].

[18] Concept developed by Jeremy Bentham. See: http://en.wikipedia.org/wiki/Panopticon

proportionality (here implied, generally recognized as having three prongs: *(i)* suitability; *(ii)* necessity; and *(iii)* non-excessiveness).

The last part of the principle refers to the awareness and informed consent of the person whose data are being collected (Article 2 (h) and Article 7 of the Directive). For the legitimate processing of their personal data, and as a general ground for lawfulness, [19] it is legally required that the involved parties give their "unambiguous and informed consent". ODR is rendered in accordance with the principle of appropriateness, which reveals the manifestation of desirable technological neutrality of the law: the same rules apply to legal relationships online and offline [33]. The general conditions for the validation of the consent are foreseen in the Directive and apply both in the offline/online world.[20] Consequently, before entering in an AmI ODR process, parties will engage in signing a "consent term"; this form is a document that brings together all the principles inherent in the process of mediation,[21] establishing itself as a formality required for the initiation of the process. It should therefore be read and signed by all parties before mediation begins.[22] In this consent form, parties are knowledgeable of the deployment of AmI technologies framework and about the potential usage of the monitoring system and how it will be used by the mediator. This implies that all this necessary information must be given at the moment the consent is requested (information addressing the substantive aspects of the processing that the consent is intended to legitimize, such as the elements of information and transparency listed in Article 10 of the Directive). Notwithstanding, concerning the validity of individual consent, the disputants will need to provide unambiguous, specific (intelligible consent that specifies the exact purpose of the processing), expressed [22] [23] and informed consent; therefore, it is patent the requirement of "granularity" of the consent[24] with regard to the different elements that constitute the data processing. To signify this consent, the data subject will deliberately fill in offline or online forms (on a contract based form) before the processing starts; it could include a handwritten signature affixed at the bottom of a paper form or by using electronic or digital signatures (through the use of "advanced electronic signature"). Regarding sensitive data, as it is our case, it is widely admitted that the signed consent is required *ad validitatem* [34]. In principle, it should be sufficient for the data controllers to obtain consent only once, according to the specific purpose of the data processing and according to the reasonable expectations of the parties. Renewed consent is not needed from the subscriber if it is guaranteed that the data in question will not be used for other purposes other than those that were defined.[25]

---

[19] Article 29 Data Protection Working Party. Opinion 15/2011 on the definition of consent.

[20] *Idem*.

[21] The alternative dispute resolution principles are stated in Directive 2008/52/EC of the European Parliament and of the Council, of 21 May 2008, on certain aspects of mediation in civil and commercial matters and on the ADR Directive (Directive 2013/11/EU); the following principles are: Transparency principle, Independence principle, Impartiality principle, Fairness principle, Effectiveness principle, Legality principle and Liberty principle.

[22] Although contract law can protect privacy within relationships formed and articulated between parties, it does not redress privacy invasions by third parties outside of the contractual bonds.

[23] The Portuguese Data Protection Authority requires a written consent.

[24] Article 29 Data Protection Working Party. Opinion 15/2011 on the definition of consent.

[25] "(...) the need for granularity in the obtaining of consent should be assessed on a case-by-case basis, depending on the purpose(s) or the recipients of data". See Article 29 Data Protection Working Party. Opinion 15/2011 on the definition of consent.

Either disputant can veto the use of the monitoring system (the so called "zero-option" or "opt in or opt out system") [21][26] and withdraw formerly given consent, at any time. It is worthy to emphasize that the knowledge gleaned during the process is destroyed once the dispute is concluded, in order to have an accountable[27] system that protects the fundamental rights of the users. The use, non-use or shift to more privacy respecting technologies remains under the discretion of each individual user[28] [21]. This right can be preserved concerning the concrete architecture and design of ODR system.[29]

In the light of the above, regarding the cognition that the ubiquitous, proactive computing systems are so embedded in daily lives that they will literally "disappear" from users consciousness [35], so that individuals will not even necessarily be conscious of their presence and will sign gladly and willingly contract clauses, consenting to the collection, cannot be envisaged nor conceived within the online mediation configuration. Conversely, under this rights-based approach, data subjects will not become de-sensitized. The technology employed in the ODR vision is accepted as being inherently control-friendly that can comprise the "reasonable expectations" of the parties, concerning their privacy [35]. On the view just presented, the potential operational data is conveyed and gathered in one specific context: only when each party accesses the ODR system, through synchronic or assynchronic communication tools, intelligent platforms and visible devices that are activated for that purpose only (each mediation session and during each mediation process); and therefore are disconnected when that mediation process is concluded.[30] These detectable devices are relatively easy-to-apply and constitute personal devices[31] [37].

We can, at some extent, concede that the obtaining of consent, in the online mediation context, is not defined in a mechanical or perfunctory manner, or as a "routinization" of consent; and this precludes the "Fallacy of Necessity" that consists in considering legitimate, justified and proportional the necessity to have an agent's consent before an action that impacts on the agent's plans and preferences [35].

---

[26] However, there are too many collectors of information for a right to opt-out to be effective. Without a centralized mechanism for individuals to opt-out, individuals would have spend much of their time guarding their privacy.

[27] Withdrawal is not retroactive, but it should, as principle, prevent any further processing of the individual´s data by the controller, Article 29 Data Protection Working Party. Opinion 15/2011 on the definition of consent.

[28] "(...)Paul Schwartz notes how consent screens on a website asking users to relinquish control over information often do so on a "take-it-or-leave-it basis" resulting in the "fiction" that people have "expressed informed consent to [the website's] data processing practices." Individuals are often presented with an all-or-nothing choice: either agree to all forms of information collection and use or to none whatsoever. Such a limited set of choices does not permit individuals to express their preferences accurately. Individuals frequently desire to consent to certain uses of their personal information, but they do not want to relinquish their information for all possible future uses (...)"[21, at 85].

[29] The ODR system, as a matter of good practice, should endeavor to review, after a certain time, the individual's choices, e.g., by offering the possibility to either confirm or withdraw. See Article 29 Data Protection Working Party. Opinion 15/2011 on the definition of consent.

[30] A basic awareness is still achievable, e.g. through clearly visible warning tags indicating that ubiquitous computing is in use.

[31] "(...) personal recording devices still lack the full surveillance capability (...).They still miss the full ability of spontaneous networking and access to data stored anywhere, and they do not possess all analytical capacities, like dataveillance, to explore the past, or profiling to generate statements and predictions about the present and the future", [37, at 145].

2.2. Data Quality Principle (paragraph 8, OECD Guidelines)

This principle computes two dimensions: *i)* the relevance of the data for the intended purpose (which locates in close relation to the further principles that we will confer); and *ii)* the exactness, completeness and topicality of the data. In order to get more accurate data, there must be regular controls and corrections as well. In this regard, each ODR advisor shall be regarded as a controller with respect to its data processing activities, in accordance with point (d) of Article 2 of the Directive, (article 12 (4) of the ODR Regulation). In this line, Article 12 (3) regarding the Regulation on ODR, establishes that personal data related to a dispute shall be kept in the ODR database only for the *time necessary* to achieve the purposes for which they were collected and to ensure that data subjects are able to access their personal data in order to exercise their rights, and shall be automatically deleted, at the latest, *6 (six) months after the date of conclusion of the dispute* which has been transmitted to the ODR platform. Thus, it is avoided the perpetuating of the appropriation of personal data.

2.3. Purpose Specification Principle (paragraph 9, OECD Guidelines)

This principle conveys the idea that at least at the time of data acquisition, the purposes are known and identifiable. In the Data Protection Directive (Article 6 (b)), it is further specified that personal data must be collected for specified, explicit and legitimate purposes. The Purpose Specification Principle is also correlated to the "Use Limitation Principle" that specifies that "personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9, except: (a) with the consent of the data subject; or (b) by the authority of law," paragraph 10 OECD, Guidelines. The legitimacy of the finality of data processing and its compatibility with these purposes can be assessed in relation to the specific and pre-definable purpose: to enrich and increase the efficiency of the communication process within a conflict resolution system with the provision of meaningful context information, and only applicable with determined and foreseeable devices. The definition of this specific purpose is the criteria for the evaluation of the lawfulness of data collection. Further, the contents and the context in which this knowledge is applied is clear at the time of collecting the data.

In our line of conceptualization, the completion of the specification purpose principle also comprises the transparency principle. The online mediator will abide to the requirements of the Directive regarding transparency of the processing of personal data. Article 10.º and 11.º demands the controller (the mediator in our case) to provide to the data subject, from whom data relating to himself are collected, with: (a) the identity of the controller; (b) the purposes of the processing for which the data are intended; (c) any further information such as the recipients or categories of recipients of the data.

The "Openness Principle"[32] is also visualized in this scenario, and is related to creating awareness about the presence of intelligent technologies. To engender online mediation in the field of ubiquitous computing systems, the release of data comprises

[32] "There should be a general policy of openness about developments, practices and policies with to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller." Paragraph 12, OECD Guidelines.

the activities the data subjects are conscious of, and therefore are, in principle, under the individual's control. The impact of online mediation AmI upon privacy is rendered evident from an analysis of particular technologies and visible terminals that are known (and some are personal) to the users (mobile devices, tactile screens and video cameras) within context-aware virtual negotiation environment, that are profile-based (in order to provide useful, non-trivial information). Moreover, it remains precise and foreseeable the moment that the monitoring system begins to operate. This substantiates our claim for the transparent extraction of features that are feasible through these devices. Hence, the knowledge derived from online mediation AmI systems matches the intentions, expectations or interests of the concerned citizen-consumers, which in term may help to mitigate information asymmetries or imbalances between the data controllers, the processors and the data subjects. It is thus evident that contextual compiled data will emerge in a transparent way to the users rather than in an unobtrusive, automatic and invisible mode.

3. Conclusions: the need for a regulatory pluralism

In this paper we suggest that the most usual criticisms to data protection envisioned in the AmI environment can be counterweighted with the specific context of ODR (within its process-centered principles and premises that are depicted in the ODR Regulation). Increasing media richness in ODR by the emotion-approach epitomizes and predicts that users will want to approach pleasant, stimulating, and controllable virtual environments and thus, emotions influence and contextual information provided by ODR processes may possibly render end-users a comfortable asset for the disclosure of their data. Even though ODR research confirms the existence of different type of services that are offered, different mechanisms employed, different IT tools used as well as the lack of interoperability services or the lack of web 2.0, web 3.0 and mobile web tools, it can be affirmed that "ODR providers understand that parties prefer to use consensual, win to win methods that entitle them to retain the ultimate decision of the controversy. Moreover, consensual methods seem to be less expensive than litigation or arbitration. Therefore, it seems that consensual-based services will increase and this seems a trend for the near future. We presume that the substantial growth of mobile penetration worldwide and some of this device's features, such as its portability, durability and relatively low-cost, suggest that mobile devices (with its incorporated sensors) might be suitable media devices.

In this article we assume that AmI leads the existing legal framework to reassess a new cognition and ponderation towards privacy and data protection law, considering the online mediation environment. The challenges of the advanced information society and the unprecedented character of a world of ubiquitous computing and ambient intelligence in an ODR scenario will mitigate and menorize the automatic collection, analysis and mining of information about the parties and contexts that may pave the way for personally–identifiable information protection, and the implied values of autonomy and self-determination.

As there is no monolithic perspective on privacy, there are multiple stake-holders and multidisciplinary endeavor in this instantiation of AmI [26]. This design conveys the proposal of relational justice, which is defined as a "bottom-up justice, produced through cooperative behavior, agreement, negotiation or dialogue" [38]. In this line, it is required adequate and matured responses from every infrastructure for fair

information practices. As such, a better regulation approach to data protection [31] would take advantage of market-based and self-regulatory institutions (including Public Law, Private Law, Soft Law, Self-Regulation, Social Norms and Technical Standards). This new approach to privacy and data protection is desirable, based on control and responsibility rather than on restriction, prohibition or "privacy myopia"[33] [39], due to the vulnerabilities affecting privacy and data protection in AmI: “the crucial issue is not the abuse but rather the fact that we have no effective means of knowing whether and when profiles are used or abused” [40]. In assessing the scope of privacy and data protection that are pertinent in the context of wearable computing, we consider transversal concern[34] [10]. A new regulatory metabolism or "regulatory pluralism" [31] including law, technology developers, ICT stakeholders and societal deliberation will need to be activated within this conceptualization of relational justice. Law and ODR may have to evolve to accommodate the new challenges raised by AmI in a communicative and evolutionist perspective. This regulatory pluralism, originating from a mainframe computer paradigm, with "built-in flexibility", can be adapted and reformed to cope with the new challenges, in order to encompass and open up the design for more privacy friendly systems and compliant tailored infrastructures.

In the present stage of research (combining AmI and ODR), it’s intricate to provide something more than simplistic and naive answers, but only modest views for the revision of EU policies and regulations, as the “Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data” (General Data Protection Regulation). The particular display of configuring ODR in AmI needs more empirical research in data protection to be fully understood, as it is necessary to be cautious about its results, since further empirical studies, tests and models are required to contrast or confirm their validity in a more general level. Nevertheless, this new advent is a promising line of research for the future of ODR.

References

1. Poblet M. and others, "Tecnologías para la mediación en línea, estado del arte, usos y propuestas", in Casanovas, P., J. Magre and M. E. Lauroba (eds), Libro Blanco de la mediación en Catalunya, Departament de Justícia, Generalitat de Catalunya edn, Huygens, 2011.
2. Poblet, M., Casanovas, P., López-Cobo, J.M., Cabrerizo, A., Prieto, J.A., Mediation, ODR, and the Web 2.0: A Case for Relational Justice. Lecture Notes in Computer Science, Vol. 6237, 2010.
3. Poblet, M., Casanovas, P., Emotions in ODR, International Review on Law, Computers, and Technology, Vol. 21(2), 2007.
4. Hammond, Anne-Marie G., How do you write “yes”? A study on the effectiveness of online dispute resolution, Conflict Resolution Quarterly, Volume 20, Issue 3, Spring 2003.
5. Ebner, Noam. ODR and Interpersonal Trust. In Wahab, Mohamed S. Abdel; Katsh, Ethan; Rainey D. (Eds.) ODR: Theory and Practice. The Hague: Eleven International Publishing, 2012, in http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2167856

[33] As Froomkin evocatively lists, "privacy myopia" consists in the fact that controllers often fail to comply with their duties under data protection laws (e.g. those arising pursuant from Articles 10 and 11 of the Directive). The author contends that data subjects suffer from inability to properly value the worth of their data in market terms, or to properly gauge the long-term significance of their consent, in terms of the impact on their privacy and autonomy [39, at 161].

[34] "(...) from the new complexities facing legal regulation of unpredictable technological developments, policy and technology have become increasingly interdependent. Legal principles, to be efficient, may need to be "embedded" in the technology itself (the development, encouraged by the European Commission, of privacy-enhancing technologies (PET’s), attests of the new distribution of regulating power between law and technology), with the implication that lawyers and engineers must engage in dialogue"[10, at 19].

6. Casanovas, P.; Poblet, M.; López-Cobo, J.M.. Relational Justice: Mediation and ODR through the World Wide Web. In F. Steiner (ed.) Archivfürrechts-und sozialphilosophie, ARSP, 2011.
7. Friedewald, M.; Vildjiounaite, E.; Punie, Y.; Wright, D., The Brave New World of Ambient Intelligence: An Analysis of Scenarios regarding Security, Security and Privacy Issues. In: Clark, J. A.; Paige, R. F. et al. (Hrsg.), Security in Pervasive Computing. Proceedings of the Third International Conference, SPC 2006, York, UK, 2006. Berlin, Heidelberg, New York: Springer (Lecture Notes in Computer Science, 3934).
8. Wahab, Mohamed S. Abdel, Does Technology Emasculate Trust? Confidentiality and Security Concerns in Online Arbitration, ICC Bulletin Special Supplement on Using Technology to Resolve Business Disputes, No. 667, 2004.
9. Andrade, Francisco, Comunicações Electrónicas e Direitos Humanos: o perigo do "homo conectus", in Direitos Humanos e sua efetivação na era da Transnacionalidade, Outubro 2012, Juruá Editora.
10. Rouvroy, Antoinette, Privacy, Data Protection and the Unprecedented Challenges of Ambient Intelligence, Studies in Ethics, Law and Technology, Vol. 2, Iss. 1, Article 3, 2008, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1013984.
11. Suquet, J; Poblet, M.; Noriega, P.; Gabarró, S., Online Dispute Resolution in 2010: a Cyberspace Odyssey? Proceedings of the 6th International Workshop on ODR 2010, CEUR Workshop Proceedings, Vol. 684, 2010.
12. Poblet M. and others, "Tecnologías para la mediación en línea, estado del arte, usos y propuestas", in Casanovas, P., J. Magre and M. E. Lauroba (eds), Libro Blanco de la mediación en Catalunya (Departament de Justícia, Generalitat de Catalunya edn, Huygens, 2011.
13. Suquet, J,"Mobile Technology and Consumer Empowerment: An Application for Online Consumer Mediation in Catalonia (Geoconsum)", European Journal for Law and Technology, Vol. 3, No. 2, 2012.
14. Poblet M., "Introduction to Mobile Technologies, Conflict Management, and ODR: Exploring Common Grounds" in Marta Poblet (ed), Mobile Technologies for Conflict Management. Online Dispute Resolution, Governance, Participation (Springer 2011).
15. Schwartz, Paul M.; Solove, Daniel J., The PII Problem: Privacy and a New Concept of Personally Identifiable Information, New York University Law Review, Vol. 86. ; UC Berkeley Public Law Research Paper No. 1909366; GWU Legal Studies Research Paper No. 584, 2011. available at SSRN: http://ssrn.com/abstract=1909366
16. Agre, Philip E.; Marc Rotenberg (eds.), Technology and Privacy. The New Landscape, MIT Press, 1998.
17. Rule, Colin, Online Dispute Resolution for Businesses. B2B, E-Commerce, Consumer, Employment, Insurance, and Other Commercial Conflicts, San Francisco, Jossey-Bass, 2002.
18. Lahlou, S, Langheinrich, M., Rocker, C., Privacy and Trust Issues with Invisible Computers, Communications of the ACM, Vol. 40, No. 3, 2005.
19. De Hert, Paul; Gutwirth, Serge; Moscibroda, Anna; Wright David; Gonzalez-Fuster, Gloria. Legal Safeguards for Privacy and Data Protection in Ambient Intelligence, http://works.bepress.com/serge_gutwirth/4/.
20. Hacking, Ian, "Making Up People", London Review of Books, 26 (16), 17 August 2007.
21. Solove, Daniel J., The Digital Person: Technology and Privacy in the Information Age, New York University Press, 2004.
22. Castro, Catarina Sarmento ,"Direito da Informática, privacidade e dados pessoais", Almedina, 2005.
23. Goldberg, Stephen B.. The Secrets of Successful Mediators, Negotiation Journal (2005) 21, 3; S.B. Goldberg & M.L. Shaw, The Secrets of Successful (and Unsuccessful) Mediators Continued: Studies 2 and 3, Negotiation Journal, 23, 2007.
24. Novais P., Carneiro D., Neves J., Incorporating Stress Estimation into User-Centred Agent-Based Platforms, in Advances on Practical Applications of Agents and Multi-Agent Systems (PAAMS 2012), Yves Demazeau, Jörg P. Müller, Juan M. Corchado Rodríguez, and Javier Bajo Pérez (Eds.), Springer - Series Advances in Intelligent and Soft Computing, vol. 155, 2012.
25. Sartor, Giovanni. Privacy, Reputation, and Trust: Some Implications for Data Protection European University Institute (EUI), Department of Law, EUI-LAW Working Papers 01/2006, in http://papers.ssrn.com/sol3/papers.cfm?abstract_id=891123
26. Jean, Camp; Kay, Connelly. "Beyond Consent", Chapter in Digital Privacy: Theory, Technologies and Practices, Alessandro Acquisti, Sabrina De Capitani di Vimercati, Stefanos Gritzalis, Costas Lambrinoudakis(eds). Auerbach Publications (Taylor and Francis Group), 2007, also available in http://www.cs.indiana.edu/~connelly/Papers/B1_BeyondConsentChapter.pdf
27. Fernando Araújo, Teoria Económica do Contrato, Almedina, 2007.
28. Benford, S.; Bullock, A; Cook, N.; Harvey, P.; Ingram, R.; Lee, O.. "From Rooms to Cyberspace: Models of Interaction in Large Virtual Computer Spaces", Interacting with Computers, Vol. 5, Issue 2, Elsevier Science, 1993.

29. Kohler, Gabrielle Kaufmann. "La resolución de los litigios en línea – perspectivas y retos del contencioso internacional contemporáneo", Revista Latino-Americana de Mediación y Arbitraje, vol. III – Nº 4, 2003.
30. Wright D.; Gutwirth S.; Friedewald M.; Punie, Y. Vildjiounaite, E., (eds.) Safeguards in a World of Ambient Intelligence, Springer Press, Dordrecht, 2008.
31. Daniel J. Solove, Nothing to Hide: The False Tradeoff between Privacy and Security, Yale University Press, 2011.
32. Winn, Jane K., Technical Standards as Data Protection Regulation, S. Gutwirth et al. (eds.) Reinventing Data Protection? Springer Science+Business Media B.V. 2009, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1118542.
33. Vicente, Dário Moura. Meios extrajudiciais de composição de litígios emergentes do comércio electrónico, in Direito da sociedade da informação, Volume V, Coimbra Editora, Coimbra, 2004.
34. Le Métayer, Daniel; Monteleone, Shara. Computer Assisted Consent for Personal Data Processing. In Proc. of 3d Conference on Legal Security and Privacy Issues in IT (LSPI'2008), p.8, in http://pop-art.inrialpes.fr/~lemetayer/lspi2008.pdf
35. Mark Weiser, Computer Science Problems in Ubiquitous Computing, Commun, ACM 36, ACM Press, 1993.
36. Brownsword, Roger, Consent in Data Protection Law: Privacy, Fair Processing, and Confidentiality. Reinventing Data Protection? Ed. Serge Gutwirth; Yves Poullet; Paul de Hert; Cecile de Terwangne; Sjaak Nouwt. Springer, 2009.
37. Cas, Johann, Ubiquitous Computing, Privacy and Data Protection: Options and Limitations to Reconcile the Unprecedented Contradictions. Computers, Privacy and Data Protection, 2011.
38. Casanovas, Pompeu; Poblet, Marta, "Concepts and Fields of Relational Justice". Computable Models of the Law, Languages, Dialogues, Games, Ontologies, 2008.
39. Bygrave, Lee Andrew; Schartum, Dag Wiese. Consent, Proportionality and Collective Power, In Serge Gutwirth; Yves Poullet; Paul De Hert; Cécile de Terwangne & Sjaak Nouwt (ed.), Reinventing Data Protection? Springer Science+Business Media B.V, 2009.
40. Hildebrandt, M., "Profiling and the identity of the European citizen." *in* Profiling the European Citizen: Cross-Disciplinary Perspectives, edited by M. Hildebrandt and S. Gutwirth. Dordrecht, Springer, 2008.
41. Carneiro D., Novais P., Andrade F., Zeleznikow J. and Neves J., Context-aware Environments for Online Dispute Resolution, in GDN 2012 - The 12th international annual meeting of the Group Decision and Negotiation conference, Recife, Brasil, 2012.