REVISTA DIREITOS SOCIAIS E POLÍTICAS PÚBLICAS (UNIFAFIBE)

DOI: http://dx.doi.org/10.25245/rdspp.v6i1.444

NEW TECHNOLOGIES AND DATA OWNERSHIP: WEARABLES AND THE EROSION OF PERSONALITY RIGHTS

TECNOLOGIAS DISRUPTIVAS, DIRECTO DE TI, DIREITOS DE PERSONALIDADE, EROSÃO DOS DIREITO DE PERSONALIDADE

Recebido em:	05/04/2018
Aprovado em:	13/06/2018

Marcos E. Kauffman [1]

Marcelo Negri Soares [2]

ABSTRACT

As technology continues to evolve at an exponentially increasing pace, it transforms our lives and societies, thus shaping our perceptions of reality with high velocity and impacting the relationship between the individual, the society, and the legal system. The young area of law known as it law is attempting to explore the effects of new technologies in our relationships with the law, as well as, identify the best use new technologies to reduce the gap between new technology, new societal behaviours and various legal systems. Therefore,

[1] PhD Researcher at Coventry University – UK; Graduate in Law LLB (Honours) at University of Buckingham – UK; Centre for Business in Society – Faculty of Business and Law; Coventry University, 113A Gosford Street, Coventry CV1 5DL. Endereço eletrônico: kauffmam@coventry.ac.uk

[2] Post Doctor in Law at UNINOVE/USP. Doctor and Master in law at PUC-SP. Law Professor at Uninove. Law Professor at PUC-Rio. Member of IBCJ and Cientist at Depac/BSGI. Researcher at the Fundação Amparo à Pesquisa do Estado de São Paulo (Fapesp). Lawyer, Accountant and Speaker. Endereço eletrônico: negri@negrisoares.com.br

REVISTA DIREITOS SOCIAIS E POLÍTICAS PÚBLICAS (UNIFAFIBE)

DOI: http://dx.doi.org/10.25245/rdspp.v6i1.444

this article aims to make a contribution to the debate by introducing and describing the current use cases of wearable technology in europe, legal issues that have been exacerbated by these emerging technologies. the article concludes that in order to mitigate the risk of erosion of personality rights new technology and innovation must to be integral components of the legal system in the future.

Keywords: disruptive technologies; technology law; personality rights; erosion of personality rights.

RESUMO

Como a tecnologia continua a evoluir num ritmo exponencialmente crescente, ela transforma nossas vidas e sociedades, moldando assim nossas percepções da realidade com alta velocidade e impactando a relação entre o indivíduo, a sociedade e o sistema legal. A jovem área de direito conhecida como TI Law está tentando explorar os efeitos das novas tecnologias em nossas relações com a lei, bem como identificar as melhores tecnologias para reduzir o hiato entre novas tecnologias, novos comportamentos sociais e vários sistemas jurídicos. Portanto, este artigo tem como objetivo contribuir para o debate, introduzindo e descrevendo os casos atuais de uso de tecnologia vestível/wearable na Europa e questões legais que foram exacerbadas por essas tecnologias emergentes. O artigo conclui que, para mitigar o risco de erosão dos direitos de personalidade, novas tecnologias e inovações devem ser componentes integrais do sistema legal no futuro.

Palavras-chave: tecnologias disruptivas; lei de tecnologia; direitos de personalidade; erosão dos direitos de personalidade.

1 INTRODUCTION

The area of Information technology law (IT Law) is a relatively new subject which has developed over the last 30 years since before the advent of the mainstream personal

REVISTA DIREITOS SOCIAIS E POLÍTICAS PÚBLICAS (UNIFAFIBE)

DOI: http://dx.doi.org/10.25245/rdspp.v6i1.444

computers (Lodder and Oskamp 2006). The area has gained momentum after the introduction of the Internet and has seen a continuous growth in the past decade with the advances in data storing, sharing and analysing over the web.

The expansion of the technologies, which enable these new internet services, leads to changes in the way people and organisation interact (Lloyd 2014), thus, giving rise to legal ambiguities and novel legal problems. Such technologies include Cloud computing, Big Data, the Internet of Things (IoT), artificial intelligence (AI), cryptography, sensors, robots, algorithms and other information related systems. Most of these technologies depend on Cloud computing infrastructures to operate at the upper level.

In a particular concept known as IoT is the key enabler for the connectivity of computing devices. IoT embraces a new concept whereby the virtual world of the Internet converges with the everyday world of "things." The idea is to connect people with each other, but also people with organisations and everyday items.

As the focal area of interest for this article is Wearable Technology which has been described by Gartner's as having surpassed the "peak of inflated expectations" and is expected to reach the "plateau of productivity" within the next decade[3]. This is yet another step in the field of miniaturization and personalization of technology, which enhances the interaction between people, devices and organisation in a multitude of ways. Due to the increasing number of wearable devices available for mass markets, wearable computing has already gained significant economic importance and will continue to do so in the foreseeable future.

[3] http://www.gartner.com/technology/research/methodologies/hype-cycle.jsp.

REVISTA DIREITOS SOCIAIS E POLÍTICAS PÚBLICAS (UNIFAFIBE)

DOI: http://dx.doi.org/10.25245/rdspp.v6i1.444

In itself, Wearables give rise to numerous legal challenges which may not be completely novel, but that will have been seen and dealt with in a limited scales and now is exponentially increased in new dimensions (Dvorak 2008). These legal questions relate areas such as data protection, copyright, contract law, trade secrets law and other regulatory aspects are most prominent. This article discusses these topics, the challenges with regard to the current legal framework, and attempts to contribute to the discussion, thoughts and bridging the gap between the between this emerging technology and the legal challenges.

There is no doubt that all these new technologies are changing the scope in which law is designed, interpreted and applied in a constantly evolving environment (Cyrul 2014). There is, therefore, an increasing global awareness that the traditional concepts and approaches to legal science must be expanded to encompass new areas associated with new technologies[4]. Based on this new reality, this work aims to provide insights on some of the key legal topics that affect our daily lives. The aim is to answer some of these questions from an inter-disciplinary and multi-jurisdictional point of view taking into account a variety of legal systems, including the EU, UK and Brazil. Therefore, we posit an approach based on generally acknowledged legal principles and thoughts rather than on the laws of a specific jurisdiction.

2 WAT DOES WEARABLE MEAN?

In order to fully appreciate the technology and its significance and impact, one must revert to basics and explore the key definition, use cases and stakeholders. As such, this section is dedicated to provide a non-technical overview of the Wearable technology.

[4] Council of Europe (1994), p. 9.

REVISTA DIREITOS SOCIAIS E POLÍTICAS PÚBLICAS (UNIFAFIBE)

DOI: http://dx.doi.org/10.25245/rdspp.v6i1.444

2.1 Wearable Technology

The concept of Wearable Technology can be defined as "the study or practice of inventing, designing, building, or using miniature body-borne computational and sensory devices."[5] These devices can be found in the form of health monitors, watches, mobile application, glasses, etc. They can also be inserted the human body itself or into almost any product, thus becoming part of us or our products. These wearable devices can be characterised by particular properties[6]. It is helpful to understand these characteristics and bear them in mind in order to fully appreciate the emanating legal challenges. As such, we provide the following non-exhaustive list which explores some of the most relevant properties of wearable devices:

A - Embedded

Term is self-explanatory, wearable technology is about devices that can be worn on or even in the body. These devices are designed to be used constantly to monitor a particular aspect or aspects of its user in almost every occasion all the time. In cases of body implants it may be difficult or even impossible to remove a wearable device from the user's body.

B - Personal

The technology focuses on personal devices. In contrast with portable and mobile technology which such as laptops, tablets and mobile phones which can be shared by

[5] Steve Mann, Wearable Computing, in: Mads Soegaard / Rikke Friis Dam (eds.), The Encyclopedia of Human-Computer Interaction, 2nd ed., 2012 (available at http://www.interactiondesign.org/
[6] Dvorak at 46/47.

REVISTA DIREITOS SOCIAIS E POLÍTICAS PÚBLICAS (UNIFAFIBE)

DOI: http://dx.doi.org/10.25245/rdspp.v6i1.444

various users, wearable devices are typically designed to be used and to monitor a single individual. As an example, artificial organs and medicine releasing devices cannot be shared with someone else, and using someone else's fitness monitor will affect the data collected and skew the information provided to the user.

C - Always present

Unlike other monitoring technologies which are fixed to a single location, Wearable devices are typically designed to be mobile and go everywhere with the user.[7] Wherever the user goes, the wearable device is, like a digital version of the user in regards to the particular aspect that it is monitoring.

D - Life logging

Unlike other devices which may be used only during working hours or during specific tasks, wearables devices as typically design to be operating or at least on standby constantly. They are in operation even during personal and intimate settings.[8] This constant data capture and monitoring is referred to as "life logging".

E - Context Aware

The wearable devices are also monitoring its environment and designed to be context aware by utilising data collected regarding its location, biomedical, and or records of its surroundings, combined in a vast amount of context aware data. In addition, the data

[7] Stephen S. Intille / Amy M. Intille, New Challenges for Privacy Law: Wearable Computers that Create Electronic Digital Diaries, MIT House_n Technical Report, September 15, 2003, at 14. 7

[8] Robert Scoble, Yes, Google Glass Survives a Wet Shower (available at https://plus.google.com/+Scobleizer/posts/TcaqNeYJWXo#+ Scobleizer/posts/TcaqNeYJWXo).

REVISTA DIREITOS SOCIAIS E POLÍTICAS PÚBLICAS (UNIFAFIBE)

DOI: http://dx.doi.org/10.25245/rdspp.v6i1.444

collected is not always obvious and/or accessible to its users and other individuals in the vicinity.

F - Decision Autonomy

Some wearable devices are designed with built in functionality for decision autonomy. Thus, the device not only to monitors the user and the surroundings, but it also processes the data collected, interpret the results and can take decisions or make suggestions on behalf of its user. Such functionality can be perceived as added value to the user in the form of increased comfort and efficiency, but it can also be seen as evidence of loss of autonomy by the user.

2.2 Wearable Devices Use Cases

After exploring the key characteristics of Wearable Technology, attention now turns to a few use cases which illustrate the operation of wearable devices. It is important to emphasise that as a rapidly evolving area of technology wearable devices are under constant development and this is an attempt to provide a non-exhaustive snapshot in time of the four key categories of wearable devices. The main purpose of the these use cases is to enlighten the source of legal challenges in relation to wearables in general and legal issues associated with particular categories of wearable devices.

I - Health and Wellbeing

There is a large range of wearable devices designed to support Health and Wellbeing use cases. These devices are aimed at various fields of application ranging from simple

REVISTA DIREITOS SOCIAIS E POLÍTICAS PÚBLICAS (UNIFAFIBE)

DOI: http://dx.doi.org/10.25245/rdspp.v6i1.444

heart rate and blood pressure monitors, all the way to highly sophisticated and intelligent devices designed to treat physical diseases and handicaps such as artificial organs[9], contact lenses[10] and diabetes glucose monitoring and control[11].

II - Sports and Fitness

There is also a wide range of devices available in this category. These include basic wearable devices which monitor and collect data such as heart rate[12], location, distance, speed, force[13], velocity and even strength during physical activities. These aim at providing information to monitor and improve the user's performance in a particular sport of fitness activity.

III - Gaming and Lifestyle

This category of devices focuses on comfort and facilitation of the user's activities. As an example, wearable input gears such as Fin[14] which facilitates the control and operation of electronic equipment, clothes equipped with digital displays[15], wristbands which utilise heart rate for user authentication[16] and finally, one of the most prominent devices in this category, the Google Glass.[17]

IV - Safety

[9] E.g. http://www.pancreum.com.
[10] See for example http://www.telegraph.co.uk/technology/google/10578729/Google-reveals-smart-contact-lens-prototype-designed-to-aid-diabetics.html
[11] https://www.dexcom.com/en-GB
[12] http://www.lumafit.com
[13] http://www.pushstrength.com
[14] http://www.wearfin.com.
[15] http://www.agentofpresence.com
[16] http://www.bionym.com
[17] http://www.google.com/glass

REVISTA DIREITOS SOCIAIS E POLÍTICAS PÚBLICAS (UNIFAFIBE)

DOI: http://dx.doi.org/10.25245/rdspp.v6i1.444

This category in turn focuses on providing its users with security and harm or damage prevention. The range of devices include the Police forces and Armed forces bodycams, firefighters equipment and even devices for vulnerable people such as baby socks[18] designed to monitor amongst other things, the baby heart rate, oxygen levels and temperature.

3 THE WEARABLE DATA OWNERSHIP AND THE IOT ECOSYSTEM

The data generated by the wearable devices is commonly uploaded at different frequencies depending in the use case and utilised in conjunction with other data sets from other devices in the IoT Ecosystem. Typically, a number of different stakeholders involved in such ecosystem, these range from device and sensor manufacturers, software and application companies, as well as, infrastructure and data analytics companies.[19]

This wide range of parties involved in the process of collecting, transferring, storing and analysing data give rise to challenges and to opportunities as "interdependencies between product and service producers" are created.[20] Therefore, as a prerequisite for such an ecosystem to function, it is often necessary to share the user's data to the various stakeholders.

3.1 Data Ownership Rights

Data ownership rights have been subject to constant debate due to the fact that businesses are increasingly valuing customer data and the insights generated from them.

[18] http://www.owletcare.com.
[19] European Commission (2016), p. 22.
[20] European Commission (2016), p. 22.

REVISTA DIREITOS SOCIAIS E POLÍTICAS PÚBLICAS (UNIFAFIBE)

DOI: http://dx.doi.org/10.25245/rdspp.v6i1.444

Questions regarding whether the companies collecting, storing, transferring, sharing and analysing data has a right to the data it processes has very often been fuelled by the lack of a clearly established right to data in the EU[21]. This section will explore the current legal position of data ownership rights in Europe and consider a few theoretical options to both, business and individuals seeking to assert their rights over data generate by wearable devices.

3.2 Property Law and Rights to Data

The area of property law is one of the most ancient systems of rights, which experts claim to predate the development of human language.[22] The concept of property and ownership thereof, concerns the regulation of tangible assets scarcity, the reality of or limited resources. [23] Such limit however, is atypical of the digital world where bits and bytes are rarely scarce and can easily be copied and multiplied without excluding others from the enjoyment of the same resource. This is commonly referred to as non rivalrous nature of data and a feature which can be found in certain Intellectual Property Law theories.[24] In this sense, data ownership, at least from a theoretical perspective, is not scarce, nor rivalrous.[25]

One of the most important aspects, if not the most important, is the right to exclude others[26] to possess the thing owned. This aspect goes to the core of Property Law and the concept of ownership, the right to possess.[27] This aspect gives rise to the first challenge

[21] European Commission (2017), p. 10.
[22] Mattei (2000), p. 4.
[23] Malgieri (2016a), p. 5.
[24] Lessig (1999), pp. 130–135.
[25] Samuelson (1999), p. 1138
[26] Clarke and Kohler (2005), p. 180.
[27] Clarke and Kohler (2005), p. 180.

REVISTA DIREITOS SOCIAIS E POLÍTICAS PÚBLICAS (UNIFAFIBE)

DOI: http://dx.doi.org/10.25245/rdspp.v6i1.444

regarding data ownership, the act of possessing "data", as such possession can be easily affected as the thing itself can be copied and replicated making it very difficult to exclude somebody else from using the same data, for cases with limited access due to technical protection.

This copy-ability of the thing owned is another challenge as a traditional aspect of any property right is the ability to exclude the world (Purtova, 2016). This aspect of property ownership is a key differentiator when compared with other rights such as rights under a contractual agreement as property rights are arguably stronger due to its enforceability everyone else, not just a contracting party.

A property right emanates from the law in vigor in a particular legal system and is independent of contractual agreements between parties. Nevertheless, the situation can be complex in certain jurisdictions as in the the case of the EU as there is no harmonisation within the EU on property law and individual rights are determined by national legislation in each of the EU Member States. Therefore, depending on the individual national rules, there may be different solutions to the legal challenges in relation to property rights to data.

An example of this lack of harmonisation can be found between the legal position in Germany, where there has been a rather extensive debate on the issue,[28] and the UK, where the courts have ruled in a case that questioned the UK position on data ownership.

In the German discussions, both civil and penal law have been used to argue in favour and against a quasi-property right to data.[29] In particular, Sect. 903 of the Civil Code

[28] Hoeren (2014).
[29] Hoeren (2014), pp. 753–754.

REVISTA DIREITOS SOCIAIS E POLÍTICAS PÚBLICAS (UNIFAFIBE)

DOI: http://dx.doi.org/10.25245/rdspp.v6i1.444

BGB regulates the ownership has not been interpreted in case law as regards data as "things," legal academics have argued that data could be recognised as a legal interest (Rechtsgut) according to the provisions that regulate liability for damages.

In the UK, the Court of Appeal had to decide if data can be subjected to liens. [30] A lien is the right of one person to retain possession of goods owned by another until the owner settles the claims by the possessor. The conclusion of the court was that despite convincing arguments to extend liens to digital material, the existing legislation could not be interpreted in such a way. The court concluded that it should be left to the Parliament to pass new law regarding digital assets.[31]

There have been other discussions by scholars on property rights, even from a privacy perspective. [32] One such discussion suggests changing the focus from tangible things to the more dynamic understanding of property as a bundle of interests.[33] Based on specific areas of law, it was argued that a property right on (personal) data could be established, while allowing individuals to both share their data as well as limit future uses of the personal data.[34] This would allow the owners of the property right a more flexible right than traditional property law.

In summary, it can be argued that no explicit property right to data is currently available in EU legislation or case law. Therefore, it follows that in order to create such right over data would demand new law or a new interpretation of the current law. In addition, even if such law existed, there are other questions regarding wearable device data in the

[30] [2014] EWCA Civ 281; [2014]3 W.L.R. 887 at Hert De and Gutwirth (2009).
[31] Kemp (2014), p. 486.
[32] Samuelson (1999).
[33] Malgieri (2016a), p. 7.
[34] Schwartz (2003), pp. 2094.

REVISTA DIREITOS SOCIAIS E POLÍTICAS PÚBLICAS (UNIFAFIBE)

DOI: http://dx.doi.org/10.25245/rdspp.v6i1.444

IoT context such as; i) who should have such right? ii) Should the right be exclusive? iii) is this right transferable?

While the challenge with traditional property law is the fact that data is not a "thing", some other rights emerging from other legal areas could be a more suitable solution to address the intangible nature of data. Some of these areas will be discussed in the next few sections.

3.3 Intellectual Property Law: Copyright in Data

Copyright is one of the potential candidates for a more suitable right over intangibles. Nevertheless, to obtain legal protection in the form of copyright, one must satisfy the requirement for originality and creativity, both international copyright conventions which establish that only works that exceed this threshold can be granted copyright protection. However, the data collected by the Wearable Technology is not "created" in the traditional sense as there is no artistic or literary work in the data, but rather, it is collected automatically from an individual or the surroundings.

Such forms of automatically collected data fail to have the required creative element of copyright,[35] as it would be impossible to demonstrate that any artistic or literary effort has been made. Furthermore, even if such creative element was found, it would arguably be the result of the user's efforts in generating the data. In this case, the user as the owners of the copyright would need to grant a license to any company using the data in the process of

[35] Article 2 Berne Convention (1886) for the Protection of Literary and Artistic Works, World Intellectual Property Organisation.

REVISTA DIREITOS SOCIAIS E POLÍTICAS PÚBLICAS (UNIFAFIBE)

DOI: http://dx.doi.org/10.25245/rdspp.v6i1.444

collecting, transferring, storing and analysing. Furthermore, in the cases where user data is paired with the surrounding data, created by external sensor and smart objects, it could be argued that companies responsible for such devices would own the copyright; for example in measuring the weather information in a particular location or even traffic, as no data individual data is being recorded. Nevertheless, wearable data would not satisfy the copyright hurdles of originality or creativity.

However, another copyright possibility lies in database rights, where legal protection is given based upon how the data is structured, rather than in the data itself. For database copyright, the database itself must pass the originality test i.e., there is originality in the selection or arrangement of the database contents. [36] Alternatively, a reduced level of protection can be given where a substantial investment in the work is shown, this is known as a sui-generis right.[37] No creativity or originality is needed here, but a sufficient level of time and effort in the structuring of data must be shown; protection can therefore even apply where a significantly large amount of data is involved.

Nevertheless, this type of protection is more likely to ensue in relation to the IoT, due to the amount of data and the time and effort involved. In any case, it is unlikely originality in the selection or arrangement of data could be shown for the database arrangements of the wearable data being collected. The sui generis right protects another party from benefiting from the result of the original investment, prohibiting the use of the whole or a substantial part of the contents. The term of protection is only 15 years, which is shorter than for copyright, but can be renewed if a new investment is made.[38] However, this

[36] Article 3 Directive 96/9/EC; Kemp (2014), p. 487.
[37] Article 7 Directive 96/9/EC.
[38] Directive 96/9/EC Article 10; the term is set at fifteen years.

REVISTA DIREITOS SOCIAIS E POLÍTICAS PÚBLICAS (UNIFAFIBE)

DOI: http://dx.doi.org/10.25245/rdspp.v6i1.444

type of rights would be likely to reside with the companies storing the data and offer no rights to the wearable device users themselves.

3.4 Contract Law

Another obvious alternative to address the lack of explicit rights to data from property law and intellectual property law, contract law can be used to guarantee a basic level of legal protection. Actually, contracts are the most common method currently in use to govern the rights and control of data between stakeholders in the IoT environment.[39] This fact is evident in the position of the European Commission which considers contracts to be "a sufficient response" to the challenges and encourages standard agreements in certain sectors.[40]

Contractual agreements offer a key advantage as they impose obligation and are enforceable against the other contracting parties. Furthermore, the standard of proof for breach of contract is less stringent than for breaches of intellectual property rights. On the other hand, a disadvantage of a right to data based on contract is that, due to privity of contract, such agreement it is only enforceable against the other contracting party, and not against any other party.[41] Thus, in a scenario relating to wearable data in complex IoT relationships between multiple parties, questions also arise in regards to which contractual agreement outweighs other terms and conditions. Furthermore, it is important to remind ourselves that contractual agreements can be overridden by other rights contained in legislation such as personal data rights and in bankruptcy proceedings.

[39] European Commission (2016), p. 21; see, e.g., for the banking sector Kemp (2014), p. 484.
[40] European Commission (2017), p. 10.
[41] Kemp (2014), p. 488.

REVISTA DIREITOS SOCIAIS E POLÍTICAS PÚBLICAS (UNIFAFIBE)

DOI: http://dx.doi.org/10.25245/rdspp.v6i1.444

4 RIGHT TO DATA: PROTECTION OF PERSONAL DATA

Most if not all of the data collected by wearable devices will relate to its users and as such, will be considered personal data. While the right to data from a business perspective is arguably unclear, the right to personal data has been enshrined in EU legislation since the Data Protection Directive (DPD) in 1995[42] and even more clearly through the recently adopted General Data Protection Regulation (GDPR) in 2016.[43]

In order to determine whether the data is characterised as personal data a basic it must be shown that the data can be linked, even if indirectly, to an individual. This link between the data and the individual has been interpreted broadly, particularly due to the term "indirectly" stated in the DPD[44] as well as the phrase: "to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person."[45] In other words, the controller does not need to be able to identify a specific person; as long as somebody can recognise a certain individual, the data is considered personal.[46] This approach was slightly adapted by the Court of Justice of the European Union (CJEU) in the recent Breyer case, as

[42] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
[43] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. The GDPR will came into force in May 2018.
[44] Definition of personal data in Article 2 (a) Directive 95/46/EC.
[45] Recital 26 Directive 95/46/EC.
[46] Article 29 Working Party (2007).

REVISTA DIREITOS SOCIAIS E POLÍTICAS PÚBLICAS (UNIFAFIBE)

DOI: http://dx.doi.org/10.25245/rdspp.v6i1.444

now the assumption is that data is considered personal data if the controller has legal means to access data that enable it to identify a specific person.[47]

The GDPR provides for a limited exception of its application in the form of anonymization. The data protection rules should "not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable."[48] Until now, the EU data protection advisory group, the Article 29 Group, has interpreted "anonymized" rather strictly and considers simply removing identifying elements as insufficient, but that the deletion of the original raw data is required as well as other technical measures to ensure that the individual cannot be re-identified.[49] In its opinion on the Internet of Things, the Article 29 Group underlined the challenges of being completely anonymous in an IoT setting and stated a clear risk of identification in the context of IoT.[50]

In conclusion, wearable device data is likely to be considered as personal data which will be processed in the IoT environment in most cases. As such, in the following sections we will discuss the rights to personal data from an individual perspective.

4.1 Privacy as a Property Right

[47] C-582/14 Patrick Breyer v Bundesrepublik Deutschland, Judgment of the Court (Second Chamber) of 19 Oct 2016.
[48] Recital 26 Regulation (EU) 2016/679, which matches Recital 26 Directive 95/46/EC.
[49] Article 29 Working Party (2014a), p. 9.
[50] Article 29 Working Party (2014a), p. 11.

REVISTA DIREITOS SOCIAIS E POLÍTICAS PÚBLICAS (UNIFAFIBE)

DOI: http://dx.doi.org/10.25245/rdspp.v6i1.444

The potential for the creation of a quasi-property right based on Privacy has been the subject of debate in Europe for almost three decades.[51] It can be argued that the intensity and frequency of these debates has increased since the turn of the century and particularly with the introduction of new technologies for data collection, transfer and analysis, as well as, the increasing value of intangible assets such as personal data to businesses, with authors such as Malgieri even arguing that personal data is a "de facto" property in today's knowledge economy (Malgieri 2016a).

Furthermore, it is argued that due to the increasing value of personal data as a new currency in the knowledge economy, the focus of EU law regarding personal data has shifted from individual privacy to the rights on the "thing" (the data). This shift arguably weakens personality rights of individuals and supports the view that data protection gives a kind of right to the data instead of protection of an individual. This view is supported by Purtova (2015) who argues that despite the fact that GDPR legislation was justified from a human-rights point of view, it nonetheless gives rise to a GDPR based property right.[52]

In the next few sections we will explore the key aspects of GDPR in relation to the new rights to data, which in our views, may be at the cost of the gradual erosion of personality rights.

4.2 The right to be forgotten

[51] Purtova (2015).
[52] Victor (2013), p. 515.

REVISTA DIREITOS SOCIAIS E POLÍTICAS PÚBLICAS (UNIFAFIBE)

DOI: http://dx.doi.org/10.25245/rdspp.v6i1.444

The GDPR creates the right to access one's personal data and also to receive information about what data is collected and stored.[53] Furthermore, it also grants an explicit right to erasure, the ("right to be forgotten").[54]

This right can be enforced in a range of circumstances, including where personal data is no longer necessary, when consent is revoked, or when the individual objects to data processing.[55] The only major exemption concerns the right to freedom of expression, which is interpreted narrowly by the CJEU in shown in the Google Spain Case.[56] As such, the individual right to be forgotten is arguably strong, as the data controller is even required to procure that other stakeholders, whom had access to the personal data, erase all the data.[57]

Thus, the right of the individual extends beyond potential contractual agreements between the wearable user and the business collecting the data, but it also encompasses other parties that have received the data. Therefore, in an IoT network, the wearable device user could for example request deletion the data by the device manufacturer, sensor manufacturer, software and application developer, infrastructure provider, and/or any data analytics companies.

As this right goes beyond the contractual rights against the parties to the contract, it can be argued that a quasi-property right as is granted by the GDPR and it overrides any contractual terms and conditions. It has been argued that the right to be forgotten is rather

[53] Article 15 Regulation (EU) 2016/679.
[54] Article 17 Regulation (EU) 2016/679. Article 12 (b) Directive 95/46/EC.
[55] See Article 17 Regulation (EU) 2016/679.
[56] Article 17.3 Regulation (EU) 2016/679. "Google Spain case": C-131/12 Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, Judgment of the Court (Grand Chamber) of 13 May 2014.
[57] Article 17.2 Regulation (EU) 2016/679

REVISTA DIREITOS SOCIAIS E POLÍTICAS PÚBLICAS (UNIFAFIBE)

DOI: http://dx.doi.org/10.25245/rdspp.v6i1.444

strong,[58] by creating a limited license to the data controllers in which it can use the individual's data, but the individual can change his/her mind at any time and break the contract by withdrawing the consent to the data.

Such strong rights, albeit useful to delete the data, arguably offer no protection to individual privacy, as once the data has been analysed and the information about the individual has been acquired and shared, it is too little, too late to delete the original data.

4.3 The Right to Data Portability

The right to data portability is another right introduced by the GDPR where an individual has the right to "receive the personal data concerning" him/her, in a structured, commonly used and machine readable format.[59] Such right was designed to allow the user to move the personal data between services and providers[60].

The right to data portability does not trigger the right to be forgotten as the two are separate rights and enforced on their own rights. In an IoT setting this means that a user can easily move between different services, for example trying out different smart health monitors and solutions, while keeping the historical data from the old device, service or provider. The application of the rights is limited to when the processing is based on the consent or a contract between the individual and the controller.[61] Nevertheless, this should be the case in most wearable devices connected to the IoT.

[58] Victor (2013), p. 524.
[59] Article 20 Regulation (EU) 2016/679.
[60] Article 29 Working Party (2016), p. 4.
[61] See Recital 68 Regulation (EU) 2016/679

REVISTA DIREITOS SOCIAIS E POLÍTICAS PÚBLICAS (UNIFAFIBE)

DOI: http://dx.doi.org/10.25245/rdspp.v6i1.444

The right to data portability, whilst not as exclusive as a property right, it still gives rise to a right to the user's data as it grants the possession of one's data as a property.

4.4 Data Protection as a Right to Data

As explored above the EU law embodied in the DPD and the GDPR grants individual rights to access to information about the data, access to the actual data, and the right to request the erasure of the data. However, a potential challenge in the IoT context is identify who has the user's data. Would the data be with the device or sensor manufacturer, software and application developer, infrastructure provider, and/or data analytics business?

Furthermore, if the data collected from a wearable device user change its status over time through anonymization or pseudonymisation techniques, the data may no longer be linked to the individual, and as such it cannot be considered personal data.

In this case, the business incentives to anonymize or pseudonomise personal data results in a diminished right to the data itself from an individual perspective, once more, arguably eroding personality rights of individuals.

CONCLUSIONS AND FUTURE DEVELOPMENT

As explored in this article, the current EU legal framework fails to provide a clear position with regards to data ownership rights. Nevertheless, there is legal protection in

REVISTA DIREITOS SOCIAIS E POLÍTICAS PÚBLICAS (UNIFAFIBE)

DOI: http://dx.doi.org/10.25245/rdspp.v6i1.444

copyright or trade secrets law or even the protection of the data as a whole in through database protection, but these are likely to apply only to businesses, which to a large degree are left to negotiate individual agreements governed by the law of contracts. These in turn, provide a strong protection against the contracting partner, but are weak against any third party who also has the data.

On the other hand, data protection rights are clearly established in EU law, particularly, when it concerns the protection of personal data and the duties of stakeholders processing such data, both of which are clearly defined in the EU law. This allows us to conclude that data protection rights are stronger than potential property rights, individual rights (including Personality Rights) and business rights, particularly as individual rights cannot be contracted away.

Nevertheless, the lack of specific property rights and the business rights to data, there are potential problems with this somewhat flexible approach, as measures implemented by businesses, such as anonymization or pseudonymisation techniques may impact on an individual's ability to access their own data and further erode his/her personality rights.

REFERENCES

Article 29 Working Party (2007) Opinion 4/2007 on the concept of personal data. Available via European Commission. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm. Accessed 16 May 2018

REVISTA DIREITOS SOCIAIS E POLÍTICAS PÚBLICAS (UNIFAFIBE)

DOI: http://dx.doi.org/10.25245/rdspp.v6i1.444

Article 29 Working Party (2012) Opinion 05/2012 on cloud computing. Available via European Commission. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinionrecommendation/index_en.htm. Accessed 16 May 2018

Article 29 Working Party (2014a) Opinion 05/2014 on anonymization techniques. Available via European Commission. http://ec.europa.eu/justice/data-protection/article-29/documentation/ opinion-recommendation/index_en.htm. Accessed 16 May 2018

Article 29 Working Party (2014b) Opinion 8/2014 on the recent developments on the internet of things. Available via European Commission. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm. Accessed 16 Jul 2017

Ashton K (2009) That 'Internet of Things' Thing. RFID Journal. 22 June 2009. http://www.rfidjournal.com/articles/pdf?4986. Accessed 17 Jan 2018

Bartolini C et al (2016) Cloud providers viability: how to address it from an IT and legal perspective? Economics of grids, clouds, systems, and services. In: Altmann J et al (eds) International Conference on Grid Economics and Business Models (GECON), Cluj-Napoca, September 2015.

Lecture notes in computer science, vol 9512. Springer International Publishing, p 281

Bradley J et al (2013) Embracing the internet of everything to capture your share of $14.4 trillion. Cisco,

REVISTA | DIREITOS SOCIAIS E POLÍTICAS PÚBLICAS (UNIFAFIBE)

DOI: http://dx.doi.org/10.25245/rdspp.v6i1.444

http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoE_Economy.pdf. Accessed 21 Jan 2018

Cisco (2013) The internet of everything and the connected athlete: this changes … everything. http://www.cisco.com/c/en/us/solutions/collateral/service-provider/mobile-internet/white_paper_c11-711705.html. Accessed 21 Jan 2018

Clarke A, Kohler P (2005) Property law: commentary and materials. Cambridge University Press, Cambridge

Custers B, Uršič H (2016) Big data and data reuse: a taxonomy of data reuse for balancing Big Data benefits and personal data protection. International Data Privacy Law 6(1):4–15

Dvorak J, Moving Wearables into the Mainstream - Taming the Borg, 2008.

Ernst and Young (2015) Becoming an analytics-driven organisation to create value. http://www.ey.com. Accessed 10 Jan 2017

European Commission (2011) Privacy and data protection impact assessment framework for RFID applications. 12 Jan 2011

European Commission (2014) Data protection impact assessment template for smart grid and smart metering systems ('DPIA template'). Expert group 2 smart grid task force. 18 Mar 2014

REVISTA DIREITOS SOCIAIS E POLÍTICAS PÚBLICAS (UNIFAFIBE)

DOI: http://dx.doi.org/10.25245/rdspp.v6i1.444

European Commission (2016) Commission staff working document, advancing the internet of things in Europe, SWD(2016) 110 final

European Commission (2017) Building a European data economy, communication from the commission to the European Parliament, the Council, The European Economic and Social

Committee and the Committee of the Regions, COM(2017) 9 final

Gartner (2016a) Forecast: wearable electronic devices, Worldwide. 19 Jan 2016

Gartner (2016b) Top strategic predictions for 2017 and beyond: surviving the storm winds of digital disruption. 14 Oct 2016

Hoeren T (2014) Big data and the ownership in data: recent developments in Europe. Eur Intellect Prop Rev 12:751–754

Kemp R (2014) Legal aspects of managing big data. Comput Law Secur Rev 30(5):482–491

Lessig L (1999) Code: and other laws of cyberspace. Basic Books, New York

Malgieri G (2016a) "Ownership" of customer (big) data in the European Union: quasi-property as comparative solution? J Internet Law 2016:3–18

Malgieri G (2016b) Trade secrets v personal data: a possible solution for balancing rights. Int Data Privacy Law 6(2):102–116

REVISTA DIREITOS SOCIAIS E POLÍTICAS PÚBLICAS (UNIFAFIBE)

DOI: http://dx.doi.org/10.25245/rdspp.v6i1.444

Mattei U (2000) Basic principles of property law: a comparative legal and economic introduction. Greenwood Publishing Group, Westport

Organisation for Economic Cooperation and Development (OECD) (2008) Committee for Information, Computer and Communications Policy (ICCP). RFID radio frequency identification OECD policy guidance: a focus on information security and privacy applications, Impacts and Country Initiatives

Purtova N (2015) The illusion of personal data as no one's property. Law Innov Technol 7(1): 83–111

Robert Scoble, Yes, Google Glass Survives a Wet Shower (available at https://plus.google.com/+Scobleizer/posts/TcaqNeYJWXo#+ Scobleizer/posts/TcaqNeYJWXo).

Samuelson P (1999) Privacy as intellectual property? Stanford Law Rev 52:1125–1151

SÁNCHES, Alcides Antúnez; SÁNCHES, Amed Ramírez. La auditoría ambiental en el derecho público de Cuba. Revista Direitos Sociais e Políticas Públicas – Unifafibe. V. 4, N. 2, 2016.

Schwartz Pa M (2003) Property, privacy and personal data. Harvard Law Rev 117:2056–2128

Stephen S. Intille / Amy M. Intille, New Challenges for Privacy Law: Wearable Computers that Create Electronic Digital Diaries, MIT House_n Technical Report, September 15, 2003

REVISTA DIREITOS SOCIAIS E POLÍTICAS PÚBLICAS (UNIFAFIBE)

DOI: http://dx.doi.org/10.25245/rdspp.v6i1.444

Victor JM (2013) The EU general data protection regulation: toward a property regime for protecting data privacy. Yale Law J 123(2):513–528

WOLF, Guilherme Eidelwein; BUFFON, Marciano. Custeio da seguridade social no Brasil: a controvérsia acerca do suposto déficit previdenciário. Revista Direitos Sociais e Políticas Públicas – Unifafibe. V. 5, N. 1, 2017.