ASSURING COMPLIANCE OF EUROPEAN SMART TOURIST DESTINATIONS WITH THE PRINCIPLES OF THE GENERAL DATA PROTECTION REGULATION, A ROADMAP[1] [2]

ASSEGURANDO O CUMPRIMENTO DOS DESTINOS TURÍSTICOS EUROPEUS INTELIGENTES COM OS PRINCÍPIOS DO REGULAMENTO GERAL DE PROTEÇÃO DE DADOS, UM ROTEIRO

Dr. Manuel David Rodrigues Masseno[3]
Dra. Cristiana Teixeira Santos[4]

Abstract: This paper aims at answering consistently to the concerns regarding privacy and personal data protection within the framework of STD that Tourism Science has put into evidence, having in mind the imminent applicability of the New General Data Protection Regulation of the EU (GDPR). Our main result renders a roadmap draft for compliance of STD design and management with the core principles embodied in the GDPR, providing guidelines both for Public and Private Sectors and for other stakeholders, namely for citizens-tourists. Our methodology is based on a strict legal analysis engaged in relevant scholarship research, but aiming for a full understating by non-Lawyers. The research is focused on 3 segments: the inherent risks related to privacy and data protection while processing personal data, the obligations of the entities processing personal data in a Smart Tourism Destination; and the possible compliance tools these entities can use to comply with the incoming regulations.We have mostly denoted the underestimation of the legal implications of technology-enhanced tourism experiences, and the marginalization of an informed involvement and awareness of tourists, as data subjects, in these processes. With this work we intend to help achieving fully Privacy compliant, in Europe and elsewhere[5].

Keywords: Privacy and Data Protection; GDPR; Regulation; Smart Tourism Destinations.

Resumo: Este trabalho tem como objetivo responder de forma consistente às preocupações em matéria de privacidade e proteção de dados pessoais no âmbito dos DTI que a Ciência do Turismo colocou em evidência, tendo em vista a iminente aplicabilidade do Novo Regulamento Geral de Proteção de Dados da EU (GDPR). O nosso principal resultado traduz um roteiro para a conformidade da concepção e gestão de DTI com os princípios fundamentais incorporados no GDPR, fornecendo orientações tanto para os Setores Público e Privado como para outras partes

1 Artigo elaborado no âmbito do Projeto de Pesquisa: "*Big Data, Cloud Computing y otros retos jurídicos planteados por las tecnologías emergentes; en particular, su incidencia en el sector turístico*" - DER2015- 63595 (MINECO/FEDER), Coordenado pela Professora Apollònia Martínez Nadal da Universitat de les Illes Balears, Espanha.

2 Estudo selecionado para o *II Congresso Mundial de Destinos Turísticos Inteligentes*, uma iniciativa da Organização Mundial do Turismo, com os Governos de Espanha e do Principado das Astúrias, realizado em Oviedo, Espanha, de 25 a 27 de junho de 2018, http://www.smartdestinationsworldconference.org/.

3 Professor Adjunto de Graduação e Mestrado e Pesquisador Sênior no Laboratório UbiNET - Segurança Informática e Cibercrime do Instituto Politécnico de Beja, Portugal. No Brasil, além de Presidente da Comissão de Direito Internacional do Cibercrime da ABCCRIM - Academia Brasileira de Ciências Criminais e Diretor para as Relações Internacionais do IBDI - Instituto Brasileiro de Direito da Informática, é Consultor das Comissões de Direito Digital e Compliance e de Legislação Aplicada à Hotelaria e ao Turismo da OAB São Paulo.

4 Graduada em Direito e Mestre em Direito dos Contratos e da Empresa, pela Universidade do Minho, Portugal. Doutorada em Direito e Tecnologia e em Informática Jurídica pelo Programa de Doutoramento Erasmus Mundus - Joint International Doctoral Degree in "Law, Science and Technology" (Universidades de Bolonha, de Turim, Autónoma de Barcelona, Mykolas Romeris de Vilnius, do Luxembrugo e de Tilburgo). Pesquisadora no JusGov - Centro de Investigação sobre Justiça e Governação da Escola de Direito da Universidade do Minho.

5 For the Legal theoretical framework of this paper, see our recently published articles, such as MASSENO, Manuel David; SANTOS, Cristiana. **Between Footprints: Balancing Environmental Sustainability and Privacy in Smart Tourism Destinations**. Unitedworld Law Journal, Vol. 1-II, 2018, pp 96-118, accessible at https://www.unitedworldschoollawjournal.com/wp-content/uploads/2018/05/Between-Footprints-Balancing-Environmental-Sustainability-and-Privacy-in-Smart-Tourism-Destinations-by-Manuel-David-Masseno-and-Cristiana-Santos-1.pdf, consulted on 15/06/2018; and also MASSENO, Manuel David & SANTOS, Cristiana. **Assuring Privacy and Data Protection within the Framework of Smart Tourism Destinations**. MediaLaws - Rivista di Diritto dei Media, 2018, 2, [Online] Available:http://www.medialaws.eu/rivista/assuring-privacy-and-data-protection-within-the-framework-of-smart-tourism-destinations/, consulted on 15/06/2018.

interessadas, nomeadamente para cidadãos-turistas. Nossa metodologia baseia-se em uma análise jurídica rigorosa envolvida em pesquisa de bolsas de estudo relevante, mas objetivando uma subavaliação completa por parte de não-advogados. A pesquisa está focada em 3 segmentos: os riscos inerentes à privacidade e proteção de dados durante o processamento de dados pessoais, as obrigações das entidades que processam dados pessoais em um Destino de Turismo Inteligente; e as possíveis ferramentas de conformidade que essas entidades podem usar para cumprir os regulamentos entrantes. Nós denotamos principalmente a subestimação das implicações legais das experiências de turismo aprimoradas pela tecnologia, e a marginalização de um envolvimento e conscientização informada dos turistas, como sujeitos de dados, nesses processos. Com este trabalho, pretendemos ajudar a alcançar a total conformidade com a privacidade, na Europa e em outros lugares.

Palavras-chave: Privacidade e Proteção de Dados; GDPR; Regulação; Destinos de Turismo Inteligente.

1 INTRODUCTION

Smart Tourism Destinations (hereinafter called STD) are an offspring of the technological foundations of *Smart Cities*, themselves benefiting from the interplay with other technological environments based on the *Internet of Things* (IoT) and the *Cloud*, as enabled by *Big Data Analytics*. However, the connections between STD and Privacy & Data Protection didn't catch a specific attention from Legal Science, even if it was perceived and pointed out as a missing issue by Tourism Science[6].

Basically, this technology enhanced tourism services allow tourists to get more from their travel and helps them fulfilling the experiential travelling potential of the destination.

But, ICT embedded within STD enable the collecting and analysis of large amounts of data, for the identification of attitude patterns and to predict their behaviors as tourists or travelers. This is achieved by addressing their potential needs and desires even at an unconscious level. Hence, theexperiences are achieved through intensive personalization, context-awareness and real-time monitoring, which consist in processes of information management that entail legal risks, demanding a careful analysis from the data protection framework. As a large spectrum of user-generated content processed in a STD concern personal data and human interaction, there is a direct impact on individuals and their rights regarding the processing of personal data.

Moreover, the application of the General Data Protection Regulation (Regulation (EU) 2016/679, hereinafter called GDPR), from the *25th May of 2018*, makes a strong case for a review of the current conceptions and practices regarding Privacy concerns STS to avoid non-compliance practices.

Nevertheless, while realizing the benefits of using big data analytics and being a competitive STD, addressing also data protection issues supports good practice in information governance that organizations purporting STD should regard closely. Therefore, data protection compliance should be an enabler of the success of STD and not a regulatory or administrative burden.

6 Namely, ANUAR, Faiz I.; GRETZEL, Ulrike. **Privacy Concerns in the Context of Location-Based Services for Tourism**. ENTER 2011 Conference. Accessibility of ICTs and Accessible Travel Information, Innsbruck, Austria, 2001, accessible at http://agrilifecdn.tamu.edu/ertr/files/2013/02/13.pdf, consulted on 15/06/2018; BUHALIS, Dimitrios; AMARANGGANA, Aditya. **Smart Tourism Destinations**. In XIANG, Zheng; TUSSYADIAH, Lis (Eds.). Information and Communication Technologies in Tourism 2014 - Proceedings of the International Conference in Dublin, Ireland. Heidelberg: Springer, 2014, pp. 553-564; or GRETZEL, Ulrike; SIGALA, Marianna *et al*. **Smart tourism: foundations and developments**. Electronic Markets, Heidelberg, Vol. 25, n. 3, 2015, pp. 179–188.

The paper is organized as follows. Section 2 provides some of the most important risks that can be appointed to STD regarding privacy and data protection. Section 3 accounts for the obligations of the organizations processing personal data, according to the General Data Protection Regulation[7], as the current basis of the Privacy and Data Protection Legal system in the European Union. Section 4refers to the compliance tools to abide with the mentioned legal obligations and Section 5 concludes the paper.

2 THE RISKS OF SMART TOURISM DESTINATIONS TO PRIVACY AND DATA PROTECTION

In this section we explain some of the potential risks STD technologies entail to Privacy and data protection. As is getting commonly known, the use and combination of advanced techniques of *Big Data Analytics*, which include machine learning (ML), data mining techniques (DM), etc., enhance the common risks hampering privacy and data protection. The following are enhanced when information (*e.g.* mobility data) is connected and matched with data from other sources of publicly available information (e.g., *Facebook* or *Twitter* postings, reviews at *Booking* or at *TripAdvisor*, blogs entries, etc.) and analysis revealed users' social interactions and activities, as for smart tourist travel cards.

2.1 Identification and re-identification of individuals from allegedly anonymized or pseudonymized data

These concerns rely on the fact that integrating large collections of data from distinct sources of available tourism datasets, even with apparently innocuous, non-obvious or anonymized resources, may enhance a jigsaw of indirect correlation of identification and re-identification; this scenario could escalate if massive information resources via the web are available[8]. Thereby, personal information set through re-identification intrinsically abides to legal requirements, as identification not only means the possibility of retrieving a person's name and/or address, but also includes potential identifiability by singling out, *linkability* and inference[9].

As data collected by the ubiquitous computing sensors is, in principle, personal data[10] or

7 Regulation (EU) 2016/679, of the EP and of the Council of 27/04/2016, 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 (General Data Protection Regulation), accessible at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG, consulted on 15/06/2018.

8 ART 29 WP – Article 29 Work Party of the European Union: Opinion 7/2003, on the re-use of public sector information, accessible at http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp83_en.pdf; Opinion 3/2013, on purpose limitation, accessible at http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf; and Opinion 6/2013, on open data and public-sector information (PSI) reuse, accessible at http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp207_en.pdf consulted on 15/06/2018.

9 ART 29 WP Opinion 05/2014, on anonymization techniques, accessible at http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf consulted on 15/06/2018.

10 ART 29 WP Opinion 4/2007, on the concept of personal data, accessible at http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf consulted on 15/06/2018.

personally identifiable information, the processing of non-sensitive data can lead, through data mining, to data that reveals personal or sensitive information, thus, blurring the conventional categories of data.

2.2 Covert profiling of individuals and non-transparency of the processing

Profiling is an important feature in tourism destinations. Tourism service providers are adapting their serviceable approach to meet the personalization expectation of costumers. In fact, data-processing scenarios collect user's input and feedback which are used to build fine-grained premium services and recommender systems in the form of trail packages. The richer the user profile, the higher the temptation for the operators to target a user with unsolicited advertising or to engineer a pricing structure designed to extract as much surplus from the user as possible[11]. Notably, "[…] analytics based on information caught in an IoT environment might enable the detection of an individual's even more detailed and complete life and behavior patterns."[12]. However, as a norm, the GDPR prohibits automated individual decision-making that significantly affect individuals, Art. 22 (1).

Indeed, developments on consumer-tourist automated profiles, facilitated by Big Data Analytics, can *significantly affect* data subjects[13]. Covert profiling, in certain cases, may lead to unintended consequences: i. when based on incomplete data, profiling can lead to false negatives, depriving individuals from benefits that they would be entitled to; ii. the so called, "*filter bubbles*" effect, according to which data subjects will only be exposed to content which confirms their own preferences and patterns, without any door open to serendipity and casual discovery; iii. isolation and/or discrimination.

Besides, within a STD, ML decisions and profiling can lead to promote direct or indirect discrimination decisions through the exclusion/denial of services/goods, e.g. denial of insurances, exclusion from the sale of touristic services or high-end products, shops or entertainment complexes to certain profiled tourists and even other decisions that reflect upon health, creditworthiness, recruitment, insurance risk, etc; it even can lead to discriminate essential utilities for those unwilling to share personal data. As we've just made clear, tourists might be discriminated against as they belong to a social group, but also such ascertainment might be based on factors, identified by the analytics, that they share with members of that group. Therefore, to ensure a fair and transparent processing (as set by the principle of fairness and transparency), automated decisions should account all the circumstances concerning the data and not be based on mere-

11 ENISA – European Networks and Information Security Agency. 2015 Report on Privacy and Data Protection by Design – from policy to engineering, accessible at https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design/at_download/fullReport consulted on 15/06/2018.

12 ART 29 WP Opinion 8/2014, on the recent developments on the Internet of Things, accessible at http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf consulted on 15/06/2018.

13 EDPS – European Data Protection Supervisor. Opinion 3/2015, Europe's big opportunity, EDPS Recommendations on the EU's options for data protection reform, accessible at https://edps.europa.eu/sites/edp/files/publication/15-10-09_gdpr_with_addendum_en.pdf consulted on 15/06/2018.

ly de-contextualized information or on data processing results[14]. Moreover, the data controller should find ways to build discrimination detection into their ML systems, to prevent inaccuracies and errors assigned to labeled profiles; as referred in Recital 71 of GDPR[15].

2.3 Repurposing of data

As data analytics can mine data for new insights and find correlations between apparently disparate datasets; hence, automatic capture of big data can be mostly reused[16] for secondary unauthorized purposes, profiling, or for abusive marketing activities, undermining the purpose specification principle convening that the purpose for which the data is collected must be specified and lawful, Art. 5(1) (b). As for a repurpose, personal data should not be further processed in a way that the data subject might consider unexpected, inappropriate or otherwise objectionable[17] and, therefore, unconnected to the delivery of the service.

2.4 Surveillance under the disguise of service provision and its desensitizing effect

On the other hand, data subject's interactions within a STD will be increasingly mediated by or delegated to (smart) devices and apps. Most of the destinations are using video-surveillance systems as sensors to supply real-time information on public transportation, traffic, also in relation to emergency and personal safety, navigation, and access to tourist information on the go, which all provide value to the user: safety, convenience, and utility in daily lives, as well as in vacation.

Such information is transmitted via, for e.g., smart remote controllable digital CCTV cameras that can zoom, move and track individual pedestrians, ANPR (number plate) recognition, GPS, Wi-Fi network tracking reliable facial recognition software, location-based service apps (LBS).

It has been argued that such devices desensitize users about providing location-based information because of the ease with which it happens and the "coolness" factor that comes with it.

2.5 Failed consent

In this sort of intelligent environments, it is problematic to give, or withhold, our prior consent to data collection, as it seems to be absent by design. The absence of awareness that the ubiquitous sensors are so embedded in the destination that they literally "disappear" from

14 ART 29 WP Guidelines on Transparency under Regulation 2016/679, accessible at http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227 consulted on 15/06/2018.

15 ART 29 WP Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, accessible at http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053 consulted on 15/06/2018.

16 ART 29 WP Opinion 3/2013, on purpose limitation, accessible at http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf (June 15, 2018).

17 COE – Council of Europe. Guidelines on the Protection of individuals with regard to the processing of personal data in a world of Big Data, T-PD, 2017, accessible at https://rm.coe.int/16806ebe7a consulted on 15/06/2018.

the users' sight. So, they will not even be conscious of their presence and hence consent to the collection. We may, at some extent, concede that the obtaining of such consent, in STD contexts, would be defined in a mechanical or perfunctory manner, or as a "routinization".

We also perceive that as for CCTV, ANPR and MAC whilst tracking and sensing, the notice in the form of information signs in the area being surveilled, or on related websites, does not conform to the consent requirements. So, the main issue of the *IoT* embedded in STD is that its sensorization devices are explicitly designed to be unobtrusive and seamless, invisible in use and unperceived to users and thereupon, users do not hold the opportunity give their unambiguous, informed, specific, explicit, and granular consent[18].

Therefore, the data controller might have difficulty in demonstrating that the consent was given, and the data subject is not able to withdraw that consent. Still, consent is not yet part of a function specification of *IoT* devices, and, thus, they do not have means to display *"*provide fine-tuned consent in line with the preferences expressed by individuals,*"* because smart roads, trams, tourist office devices are usually small, screenless and lack an input mechanism (a keyboard or a touch screen)[19].

2.6 Imbalance

Smart technologies often produce situations of imbalance, where data subjects are not aware of the fundamental elements of data processing and related consequences, being unable to negotiate their information, which leads to a side consequence of an enhanced information asymmetry as consumers.

2.7 Tendency to collect and analyze all data

The tourism industry is inherently based on data-exchange: to generate massive databases, is necessary to optimally exploit all information available and as so, datasets need to be exhaustive and varied as possible to faithfully reflect the touristic activity of a territory.

In substance, smart technology purports the extensive collection, aggregation and algorithmic analysis of all the available data for various reasons, such as understanding customer buying behaviours and patterns or remarketing based on intelligent analytics, hampering the data minimization principle (Art. 5 (1)(c). In addition, irrelevant data is being also being collected and archived, undermining the storage limitation principle (Art. 5 (1) (e).

18 ART 29WP Opinion 15/2011, on the definition of consent, accessible at http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf consulted on 15/06/2018; updated by its Guidelines on Consent under Regulation 2016/679, accessible at http://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51030 consulted on 15/06/2018.

19 ART 29 WP Opinion 8/2014, on the recent developments on the Internet of Things, accessible at http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf consulted on 15/06/2018.

2.8 Inaccurate data

Results drawn from data analysis may not be representative or accurate, if sources aren´t trustworthy as well (*i.e.*, analysis based on social media resources are not necessarily representative of the whole population at stake).

Besides, machine learning itself may contain hidden bias which lead to inaccurate predictions and profiles about individuals. In any case, profiling implicates creating derived or inferred data, occasionally leading to incorrect decisions (discriminatory, erroneous and unjustified, regarding their behaviour, health, creditworthiness, recruitment, insurance risk, etc.).

Even exercising the "*right to be forgotten*", where data subjects will have the right for their data to be erased in several situations, for e.g., when the data is no longer necessary for the purpose for which it was collected, or based on inaccurate data (as set by the accuracy principle depicted in Art. 5 (1) (d). In fact, it may be difficult for a business to find and erase someone's data if it is stored across several different systems and jurisdictions.

3 THE OBLIGATIONS OF ORGANIZATIONS WHILE PROCESSING PERSONAL DATA WITHIN A STD

While realizing the benefits of using big data analytics and being competitive STD, addressing also data protection concerns supports best practices in information governance that organizations purporting STD should regard closely. Data protection compliance should hence be an enabler of the success of STD and not a regulatory or procedural burden. As almost everybody in Europe is now aware, an infringement or non-compliance with the Regulation may lead to fines up to €20 million, or 4% of the worldwide annual revenue of the prior financial year, whichever is higher.

As stated in the tourism literature, tourism, by definition, is a service-intense industry with a "*business network*", since it relies on a number of stakeholders for its ability to deliver products and services. In this network, each of the actors involved in the transportation, accommodation, gastronomy, attractions and ancillaries' services, potentially process personal data.

For a STD, the public or private organisations that decides "why" and "how" the personal data should be processed are called as "data controllers". They might use other parties that process personal data on their behalf, called "data processors". Both data controller and data processors must abide to the GDPR obligations.

However, Big Bata Analytics can make it difficult to discern between controllers and processors; further, within the modern data value chain, organizations outsourcing analytics and AI to specialized companies need to consider carefully who has control over the processing of any personal data, Art. 4 (7) (8).

Therefore, if an organization chooses to store its customer data in the cloud, then the cloud provider is likely to be a data processor, as it is acting on the original organization's behalf, and he is not determining the purposes of the processing.

Hence, if an organization purports to conduct its analytics outsourcing in a data controller-data processor relationship, it is important that the contract includes clear instructions about how the data can be used and the specific purposes for its processing. However, the existence of such a contract does not entail that the sub-contracted company performing data analysis is a data processor; if this company uses its discretion and expertise to decide what data to collect and how to apply its analytic techniques, then it is very likely to be a data controller as well, actually a co-controllership[20] (Art. 24).

Under the accountability principle (Art. 24) data controllers shall be responsible for, and be able to demonstrate compliance with all the obligations and principles contained in the regulation; some of the most important obligations are herewith explained.

3.1 Appointing a Data Protection Officer

The GDPR mandates the appointing of a Data Protection Officer (DPO) within the organization whose responsibilities include monitoring data governance and privacy; and will offer advice, monitor data protection impact assessments and act as the point of contact with any supervisory authority. This is mandatory where the processing is carried out by a public authority or body, except for the courts; their core activities consist of processing operations which require regular and systematic monitoring of data subjects on a large scale, or processing on a large scale of special categories of data (Articles 37 to 39)[21].

3.2 Algorithmic accountability

Organizations should also check "algorithmic accountability", which means being able to check that the algorithms used and developed by machine learning (ML) systems are actually doing what we think they're doing and aren't producing discriminatory, erroneous or unjustified results. Organizations using ML techniques in STD need to assure a compliance function of data quality by checking the sources of the data, the accuracy of the data, whether is sufficiently up to date, how securely it is kept, and whether there are restrictions on how it can be used (anonymised data).

20 ICO Guide on Big Data, Artificial Intelligence, Machine Learning and Data Protection, 2017, accessible at https://ico.org.uk/for-organisations/guide-to-data-protection/big-data/ consulted on 15/06/2018.

21 ART 29 WP Guidelines on Data Protection Officers ('DPOs'), accessible at http://ec.europa.eu/newsroom/document.cfm?doc_id=44100 consulted on 15/06/2018.

3.3 Fair, lawful and transparent processing obligation

STD organizations must process personal data in a "fairly, lawfully and in a transparent manner in relation to the data subject", i.e. when the data is collected, it must be clear as to why that data is being collected and how the data will be used. Whether the data are volunteered, observed, or inferred, or collected from accessible sources, individuals are fully entitled to know which are they, from where and from whom the controllers obtained it, and how automated decisions were taken. The GDPR prohibits automated individual decision-making that significantly affect individuals, Art. 22 (1). Therefore, in order to ensure a fair and transparent processing, automated decisions should account all the circumstances concerning the data and not be based on merely de-contextualized information or on data processing results. In furtherance of this aim, the controller should find ways to build discrimination detection into their ML systems, to prevent inaccuracies and errors assigned to labeled profiles.

3.4 Lawfulness of processing

Processing personal data should be grounded on some conditions, namely: the consent of the tourist, a contract, a public interest, a legitimate interest, etc. In these intelligent environments, it is dubious to give or withhold our prior **consent** to data collection, as it seems to be absent by design. The awareness that the ubiquitous sensors are so embedded in the destination that they literally "disappear" from the users' sight, so that they will not even be conscious of their presence and hence consent to the collection, can be envisaged within STD. So, at some extent, the obtaining of such consent, in STD contexts, would be defined in a mechanical or perfunctory manner, or as a "routinization".

Reverting also to other legal grounds, processing personal data relies on "**public interest**", which can sidestep the need for consent (health, national governmental agencies gather data for e. g. e-Government systems, e-Health). Nevertheless, this possibility should not conceal any eventual "third-party interest".

Most commercial systems rely on the "**legitimate interests**" ground, even if they consist in "the vaguest ground for processing", and offers a lot of scope for industry to process data by claiming any deemed necessary "legitimate interest". In fact, the processing must be "necessary" for the legitimate interests and not just *potentially* interesting. It follows that the processing is not necessary if there is any other way of meeting the legitimate interest that interferes less with the people's privacy.

As for the contractual condition, it may be difficult to show that big data analytics in STD are strictly necessary for the performance of a **contract**, since the processing goes beyond what is required to sell a product or deliver a service.

3.5 Purpose limitation

The principle purpose limitation utters that the purpose for which the data is collected must be specified and lawful. This principle also prevents arbitrary reuse, which means that personal data should not be further processed in a way that the data subject might considered on unexpected, inappropriate or otherwise objectionable and therefore unconnected to the delivery of the service; concretizing, by exposing data subjects to different/greater risks than those contemplated by the initial purposes could be considered as a case of further processing of data in an unexpected manner[22].

3.6 Data Minimization, Collection and Retention obligations

Data minimization means that personal data shall be "*adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed*" Art. 5 (1) (c), and such obligation means that STD entities should minimize the amount of data they collect and process, and the length of time they keep the data. Even if in practice, smart technology purports the massive collection, aggregation and algorithmic analysis of all the available data to understand customer buying behaviors and patterns or remarketing based on intelligent analytics, organizations need to be clear about which data is deemed to be *necessary, excessive* and *relevant* for the purposes of the processing. As for data storage, personal data shall not be kept (stored) longer than necessary for the purpose for which it is being processed, as prescribed by the storage limitation principle, Art. 5 (1) (e). This obligation is part of the lifecycle governance strategy retention policies of companies that defensibly dispose irrelevant data instead of keeping data archived forever. Regarding retention timeframes, retention schedules allow unnecessary data to be disposed of as it is no longer of business value or needed to meet legal obligations. Data mapping techniques are welcome to identify where and what type of data is stored within an organization. Data management segmentation can also help to segregate EU data from data coming from other data subjects.

3.7 Accuracy and up to date processing obligations

If sources of data are reliable, accurate and representative, so the results drawn from big data analysis employed in a STD environment (Art. 5 (1) (d)), e.g. analysis based on social media resources are not necessarily representative of the whole population at stake[23]. Organizations employing ML algorithms need to consider the distinction between correlations and causations[24], *i.e.*, when there is no *direct cause and effect* between two phenomena that show a close cor-

22 ART 29 WP Opinion 3/2013, on purpose limitation, accessible at http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf consulted on 15/06/2018.

23 ICO Guide on Big Data, Artificial Intelligence, Machine Learning and Data Protection, 2017, accessible at https://ico.org.uk/for-organisations/guide-to-data-protection/big-data/ consulted on 15/06/2018.

24 ICO Guide on Big Data, Artificial Intelligence, cit.

relation. In these cases there is a risk of drawing inaccurate, but also – and when applied at the individual strata – potentially unfair and discriminatory conclusions[25].The potential accuracy (or inaccuracy) of any resulting decisions might cause discriminatory, erroneous and unjustified decisions, regarding data subject´s behavior on health, creditworthiness, recruitment, insurance risk, etc. The quality of the profiles and the quality of personal data on which they are built, again, seem to matter for the prosperity of the industry.

3.8 Data breach reporting

EU data protection law requires controllers to notify the relevant supervisory authority and the data subjects of potential data breaches in the event of causing high risk to data subjects, without undue delay. The notification must include at least: the name and contact details of the DPO (or other relevant point of contact); the likely consequences of the data breach; and any measures taken by the controller to remedy or mitigate the breach. However, the controller may be exempt from this requirement if the risk of harm is remote because the affected data are protected (e.g., through strong encryption). Most importantly, if the risks associated with the breach have been effectively resolved then the organisation may be exempt from the notification requirements[26].

3.9 Processing activities records

EU data protection law requires organizations involved in STD to keep records (written or electronic) of their data processing activities (Art.30), e.g. the purposes of the processing; the categories of data subjects and personal data processed; the categories of recipients with whom the data may be shared. Upon request, these records must be disclosed to DPAs.

3.10 Codes of conduct and certification mechanism

In order to enhance transparency and compliance with this Regulation, associations and other institutional bodies representing both controllers and processors are compelled to elaborate codes of practice specifying how the GDPR should be applied. Then, these bodies must submit their draft codes of conduct to the relevant supervisory authority for approval. The GDPR introduced certification mechanisms and data protection marks, allowing data subjects to quickly assess the level of data protection of relevant products and services. A list of certified organizations will be hence publicly available. Codes of conduct and approved certification mechanisms will also assist controllers, in identifying the risks related to their type of processing and in adhering to best practice.

25 EDPS Opinion 7/2015 on Meeting the challenges of big data, accessible at https://edps.europa.eu/sites/edp/files/publication/15-11-19_big_data_en.pdf consulted on 15/06/2018.

26 ART 29 WP Guidelines on Personal data breach notification under Regulation 2016/679, accessible at http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052 consulted on 15/06/2018.

4 COMPLIANCE TOOLS AT THE GDPR

Compliance tools enable STD organizations meeting their data protection obligations while protecting people's privacy rights in a STD context, and they are: anonymization and pseudonymization techniques, privacy policies, data protection impact assessment (DPIA), personal data stores, algorithmic transparency, privacy seals/certification, and privacy by design (PbD) measures to mitigate the appointed legal risks and implications. STD managers could deploy internally documentation and training activities by training employees on the GDPR-related mandates and distributing written internal policies to demonstrate commitment to compliance.

4.1 Anonymization

As a stated principle, when data is rendered *anonymous* (Recital 26 of the GDPR) all identifying elements have been irreversibly eliminated from a set of personal data, and cannot leave space to re-identify the person(s) concerned; therefore, it is deemed to be no longer personal data. Later, anonymised data might be aggregated to be analysed and to gain insights about the population, as well as combined with data from any other sources. At this stage, *IoT* developers can analyse, share, sell or publish the data without data protection requirements.

Conversely, de-anonymization strategies in DM entails that anonymous data is cross-referenced with other sources to re-identify the anonymous data. Thus, the processing of datasets rendered anonymous may never be absolutely ensured.

In what refers to *pseudonymized* personal data, identifiers are replaced by a pseudonym (through encryption of the identifiers). In turn, pseudonymized data continues to allow an individual data subject to be singled out and linkable across different datasets and therefore stays inside the scope of the legal regime of data protection[27].

4.2 Privacy policies

Privacy policies consist of multiple paragraphs of natural language disclosing an organization's data practices on processing activities of personal data to its users, such as collection, use, sharing, and retention. They serve as a basis for decision-making, a "tool for preference-matching" for consumers, as they tend to value a product/service more, after learning more about its attributes and tradeoffs for making a consumption decision. As such, they constitute the locus where consequences are produced, the "technically most feasible place to protect privacy and personal data.

The GDPR states that information addressed to the data subject should be "concise, easily accessible and easy to understand, and that clear and plain language, and additionally, where

27 ART 29 WP Opinion 05/2014, on anonymization techniques, accessible at http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf consulted on 15/06/2018.

appropriate, visualization is used", Article 12(7) and Recital 60.

However, in a STD scenario, these requirements can be problematic, and it has been suggested that privacy notices are not feasible when Big Data Analytics perform, by reason of: travelers engaged in tourism experiences are unwilling to read lengthy legalese privacy notices, since it would take significantly more time than they spend using the content or the app; the context in which data is collected (e.g., destination apps, wearable watches and glasses or IoT devices) is difficult to provide the information.

Regarding the amount and assortment of these interactions, it is just too onerous for each data subject to assess their privacy settings across dozens of entities, if any, in order to ponder about the non-negotiable tradeoffs of agreeing to privacy policies without knowing how the data might be used now and in the future, and to assess the cumulative effects of their data being merged with other datasets. On the other hand, information can be delivered in a user-friendly form, namely by videos or in-app notices; cartoons and standard icons applied to privacy notices, explaining their content; as for wearable devices, privacy information could be provided on the device itself, or by broadcasting the information via Wi-Fi or making it available through a QR code[28].

4.3 Data protection impact assessment

A data protection impact assessment (DPIA) is a tool that can help to identify and mitigate privacy risks, before the processing of personal data. This assessment involves description of the envisaged processing operations, an evaluation of the privacy risks and the measures envisaged to address those risks.

Art. 35 of GDPR denotes that when a type of processing resorting to a systematic and extensive evaluation of individuals based on automated processing and profiling, significantly affecting individuals using new technologies, and when such a processing is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged operations on the protection of personal data. So, it is most likely that general big data applications involving the processing of personal data, within a STD, will fall into this category[29].

4.4 Privacy by design

By design solutions (PbD) consist in an approach in which IT system designers should code both preemptive *technological* and *organizational* measures to protect personal data, when conceiving specifications of new products and services. By design solutions are necessary at the early development stage (planning and implementation) of any new product or service that affects personal data. It aims to address privacy concerns applied to the very same technology that

28 ART 29 WP Opinion 8/2014, on the recent developments on the Internet of Things, accessible at http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf consulted on 15/06/2018.

29 ART 29 WP Guidelines on Data Protection Impact Assessment (DPIA), accessible at http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236 consulted on 15/06/2018.

might create risks (Art. 25). Besides anonymization techniques, PbD involves other engineering and organizational measures, including: security measures such as access controls, audit logs and encryption; data minimization measures, to ensure that only the personal data that is needed for a particular analysis or transaction is processed at each step (such as validating a customer);purpose limitation and data segregation measures so that, for example, personal data is kept separately from data used for processing intended to detect general trends and correlations; and, sticky policies' that record individual's preferences and corporate rules within the metadata that accompanies data.

At a STD scenario, controllers and processors should test the adequacy of the above-mentioned solutions by-design on a limited amount of data by means of simulations before their use on larger scales, in a learn-from-experience approach. This would make it possible to assess the potential bias of the use of different parameters in analyzing data and provide evidence to minimize the use of information. However, there is a lack of a privacy mindset in IT system designers, as stated by ENISA:

> […] *privacy and data protection features are, on the whole, ignored by traditional engineering approaches when implementing the desired functionality. This ignorance is caused and supported by limitations of awareness and understanding of developers and data controllers as well as lacking tools to realize privacy by design. While the research community is very active and growing, and constantly improving existing and contributing further building blocks, it is only loosely interlinked with practice*.[30]

4.5 Personal data spaces

The European Data Protection Supervisor suggested that one way to increase an individual's control over the use of their data is through what are usually called personal data spaces, vaults or stores, also denominated by personal information management services[31]. These are third-party services (intermediaries) that collect, manage and store people's personal data on their behalf and make it available to organisations as and when the individuals wish to do so. This tool aims to address the critics related to the lack of control of how personal data is used in a big data environment, as tourists are not aware of how data is being collected or how it is used, and don't have the time to read privacy notices.

4.6 Algorithmic transparency

Namely, the following suggestions on the view of algorithmic transparency are reflected in the findings of research of the Information Commissioner´s Office of the UK[32]: Techniques for algorithmic auditing can be used to identify the factors and make transparent the algorithm step-

30 ENISA 2015 Report on Privacy and Data Protection by Design – from policy to engineering, accessible at https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design/at_download/fullReport consulted on 15/06/2018.

31 EDPS Opinion 7/2015 on Meeting the challenges of big data, accessible at https://edps.europa.eu/sites/edp/files/publication/15-11-19_big_data_en.pdf consulted on 15/06/2018.

32 ICO Guide on Big Data, Artificial Intelligence, Machine Learning and Data Protection, 2017, accessible at https://ico.org.uk/for-organisations/guide-to-data-protection/big-data/ consulted on 15/06/2018.

by-step development that influence an algorithmic decision and assure public trust; Interactive visualization systems can help individuals to understand why a recommendation was made and give them control over future recommendations; and, Ethics boards can be used to help shape and improve the transparency of the development of machine learning algorithms.

4.7 Privacy seals and certification

Certification schemes (Arts. 42, 43, Recital 100) can be used to help demonstrating data protection compliance of STD big data processing operations. They encourage the "establishment of data protection certification mechanisms and of data protection seals and marks" to demonstrate that processing operations comply with the Regulation. These would be awarded by data protection authorities or by accredited certification bodies[33].

5 CONCLUSIONS

The preceding analysis brings out that smart tourism is becoming a big contributor and benefactor of ubiquitous, always-on data capture about customers towards enhanced tourism experiences, and competitive markets. This extensive collection and processing of personal data in the context of STD using algorithm-driven techniques has given rise to serious privacy concerns, especially relating to the wide ranging electronic surveillance, profiling, and disclosure of private data. The apprehension here is to understand if the affordances of the technology, the personalized services, and enhanced experiences can cope with data protection obligations without such a micro-targeting and profiling. As we have seen, Smart Tourism raises big issues with respect to information governance and about correctly deriving the "added" value from information in an open and ubiquitous info-structure. And, even if European SDT were already under Data Protection regulation, both from the EU and national, the new GDPR will be a real game changer, to be compliant with, without further excuses.

REFERENCES

Namely, ANUAR, Faiz I.; GRETZEL, Ulrike. **Privacy Concerns in the Context of Location-Based Services for Tourism**. ENTER 2011 Conference. Accessibility of ICTs and Accessible Travel Information, Innsbruck, Austria, 2001, accessible at http://agrilifecdn.tamu.edu/ertr/files/2013/02/13.pdf, consulted on 15/06/2018; BUHALIS, Dimitrios; AMARANGGANA, Aditya. **Smart Tourism Destinations**. In XIANG, Zheng; TUSSYADIAH, Lis (Eds.). Information and Communication Technologies in Tourism 2014 - Proceedings of the International Conference in Dublin, Ireland. Heidelberg: Springer, 2014, pp. 553-564; or GRETZEL, Ulrike; SIGALA, Marianna et al. **Smart tourism:** foundations and developments. Electronic Markets, Heidelberg, Vol. 25, n. 3, 2015, pp. 179–188.

33 ENISA 2017 Recommendations on European Data Protection Certification, accessible at https://www.enisa.europa.eu/publications/recommendations-on-european-data-protection-certification/at_download/fullReport consulted on 15/06/2018.

Regulation (EU) 2016/679, of the EP and of the Council of 27/04/2016, 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 (General Data Protection Regulation), accessible at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG, consulted on 15/06/2018.

ART 29 WP – Article 29 Work Party of the European Union: Opinion 7/2003, on the re-use of public sector information, accessible at http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp83_en.pdf; Opinion 3/2013, on purpose limitation, accessible at http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf; and Opinion 6/2013, on open data and public-sector information (PSI) reuse, accessible at http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp207_en.pdf consulted on 15/06/2018.

ART 29 WP Opinion 05/2014, on anonymization techniques, accessible at http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf consulted on 15/06/2018.

ART 29 WP Opinion 4/2007, on the concept of personal data, accessible at http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf consulted on 15/06/2018.

ENISA – European Networks and Information Security Agency. 2015 Report on Privacy and Data Protection by Design – from policy to engineering, accessible at https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design/at_download/fullReport consulted on 15/06/2018.

ART 29 WP Opinion 8/2014, on the recent developments on the Internet of Things, accessible at http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf consulted on 15/06/2018.

EDPS – European Data Protection Supervisor. Opinion 3/2015, Europe's big opportunity, EDPS Recommendations on the EU's options for data protection reform, accessible at https://edps.europa.eu/sites/edp/files/publication/15-10-09_gdpr_with_addendum_en.pdf consulted on 15/06/2018.

ART 29 WP Guidelines on Transparency under Regulation 2016/679, accessible at http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227 consulted on 15/06/2018.

ART 29 WP Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, accessible at http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053 consulted on 15/06/2018.

ART 29 WP Opinion 3/2013, on purpose limitation, accessible at http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf (June 15, 2018).

COE – Council of Europe. Guidelines on the Protection of individuals with regard to the processing of personal data in a world of Big Data, T-PD, 2017, accessible at https://rm.coe.int/16806ebe7a consulted on 15/06/2018.

ART 29WP Opinion 15/2011, on the definition of consent, accessible at http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf consulted on 15/06/2018; updated by its Guidelines on Consent under Regulation 2016/679, accessible at http://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51030 consulted on 15/06/2018.

ART 29 WP Opinion 8/2014, on the recent developments on the Internet of Things, accessible at http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf consulted on 15/06/2018.

ICO Guide on Big Data, Artificial Intelligence, Machine Learning and Data Protection, 2017, accessible at https://ico.org.uk/for-organisations/guide-to-data-protection/big-data/ consulted on 15/06/2018.

ART 29 WP Guidelines on Data Protection Officers ('DPOs'), accessible at http://ec.europa.eu/newsroom/document.cfm?doc_id=44100 consulted on 15/06/2018.

ART 29 WP Opinion 3/2013, on purpose limitation, accessible at http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf consulted on 15/06/2018.

ICO Guide on Big Data, Artificial Intelligence, Machine Learning and Data Protection, 2017, accessible at https://ico.org.uk/for-organisations/guide-to-data-protection/big-data/ consulted on 15/06/2018.

ICO Guide on Big Data, Artificial Intelligence, cit. EDPS Opinion 7/2015 on Meeting the challenges of big data, accessible at https://edps.europa.eu/sites/edp/files/publication/15-11-19_big_data_en.pdf consulted on 15/06/2018.

ART 29 WP Guidelines on Personal data breach notification under Regulation 2016/679, accessible at http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052 consulted on 15/06/2018.

ART 29 WP Opinion 05/2014, on anonymization techniques, accessible at http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf consulted on 15/06/2018.

ART 29 WP Opinion 8/2014, on the recent developments on the Internet of Things, accessible at http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf consulted on 15/06/2018.

ART 29 WP Guidelines on Data Protection Impact Assessment (DPIA), accessible at http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236 consulted on 15/06/2018.

ENISA 2015 Report on Privacy and Data Protection by Design – from policy to engineering, accessible at https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design/at_download/fullReport consulted on 15/06/2018.

EDPS Opinion 7/2015 on Meeting the challenges of big data, accessible at https://edps.europa.

eu/sites/edp/files/publication/15-11-19_big_data_en.pdf consulted on 15/06/2018.

ICO Guide on Big Data, Artificial Intelligence, Machine Learning and Data Protection, 2017, accessible at https://ico.org.uk/for-organisations/guide-to-data-protection/big-data/ consulted on 15/06/2018.

ENISA 2017 Recommendations on European Data Protection Certification, accessible at https://www.enisa.europa.eu/publications/recommendations-on-european-data-protection-certification/at_download/fullReport consulted on 15/06/2018.

Recebido: 18 de junho de 2018
Aprovado: 07 de agosto de 2018

LA PROMOZIONE DELL'ENERGIA DA FONTI RINNOVABILI: IL QUADRO NORMATIVO ITALIANO ED INTERNAZIONALE

THE PROMOTION OF ENERGY FROM RENEWABLE SOURCES: THE ITALIAN AND INTERNATIONAL REGULATORY FRAMEWORK

Dr. Luigi Benvenuti[1]
Me. Jamila Wisóski Moysés Etchezar[2]

RIASSUNTO: Questo articolo si occupa in particolare di una delle questioni più attuali, anche in tutto il mondo, in materia di diritto ambientale e di diritto pubblico, cioè "la disciplina delle energie rinnovabili". L'argomento, come accennato, coinvolge l'intera comunità mondiale, e in particolare l'Italia, che nel referendum del 2011 giugno ha scelto di non utilizzare l'energia nucleare. Una scelta che implicitamente significava anche l'aderenza ad un futuro uso dell'energia da fonti rinnovabili. L'adozione dell'aggettivo "futuro" significa che l'Italia non è ancora in grado di utilizzare le energie rinnovabili come unica fonte di approvvigionamento energetico. La discussione si concentrerà inoltre sul collegamento degli impianti di produzione di biogas alla rete del gas naturale e sull'incentivazione del biometano nella rete del gas naturale, nonché su il quadro normativo internazionali e sui principi fondamentali in materia ambientale.
Parole chiave: Ambiente. Fonti Rinnovabili. Energie Rinnovabili. Norme Internazionali.

ABSTRACT: This article deals in particular with one of the most current issues, also around the world, in the field of environmental law and public law, i.e. "the discipline of renewable energies". The argument, as mentioned, involves the entire world community, and in particular Italy, which in the referendum of 2011 June chose not to use nuclear energy. A choice that implicitly meant also adherence to a future use of energy from renewable sources. The adoption of the adjective "future" means that Italy is not yet able to use renewable energies as the only source of energy supply. The discussion will also focus on the connection of biogas production plants to the natural gas network and the stimulation of biomethane in the natural gas network, as well as on international standards and on the fundamental principles Environmental.
Keywords: Environment. Renewable Sources. Renewable. International Standards.

1 PREMESSA

Il Decreto Legislativo Italiano del 3 marzo 2011, n. 28[3] esordisce dichiarando chiaramente le proprie finalità: l'art. 1 del D.Lgs. n. 28/2011, infatti, lungi dal contenere norme di carattere precettivo, si presenta come una sorta di dichiarazione di intenti, avente ad oggetto il raggiungimento degli obiettivi fissati a livello europeo per l'anno 2020 in materia di consumo di energia da fonti rinnovabili, e quindi la predisposizione dei necessari strumenti, meccanismi,

1 Membro del Collegio docenti de Master in Diritto dell´Ambiente dell´Università Ca' Foscari. Cordinatore del Dottorato in Diritto Europeo dei Contratti civili, comerciali e del lavoro dell´Università Ca' Foscari di Venezia. Email: luigi.benvenuti@unive.it

2 Master nel diritto ambientale dell'Università Cà Foscari di Venezia (2011). Laurea specialistica in scienze giuridiche e sociali presso all'Università di Passo Fundo (2007). Professore di diritto presso le Facoltá Giovanni Paolo II in PassoFundo, RS. email: juridicapassofundo@hotmail.com

3 Il Decreto Legislativo 3 marzo 2011, n. 28, "Attuazione della direttiva 2009/28/CE sulla promozione dell'uso dell'energia da fonti rinnovabili, recante modifica e successiva abrogazione delle direttive 2001/77/CE e 2003/30/CE", è entrato in vigore il 29 marzo 2011, è pubblicato in Gazzetta Ufficiale n. 71, 28 marzo 2011, Supplemento Ordinario n. 81, è reperibile al sito http://www.governo.it/Governo/Provvedimenti/testo_int.asp?d=62612 consultato il 19 agosto 2011.