UNIVERSITÀ
DEGLI STUDI
DI PADOVA

Università degli Studi di Padova

Dipartimento di Studi Linguistici e Letterari

Corso di Laurea Magistrale in
Lingue Moderne per la Comunicazione e la Cooperazione Internazionale
Classe LM-38

Tesi di laurea

The role of digital technologies on climate protection: a matter of inner oppositions

Relatore
Prof. Nicola Brutti

Anno Accademico 2021 / 2022

Laureanda
Elena Zanetti
n° matr.2017275 / LMLCC

"You want to prevent the privacy harms from arising, not just resolve them after the fact, you want to prevent them."[1]

A mamma e papà

[1] Dr. Ann Cavoukian, the former Information and Privacy Commissioner for the Canadian province of Ontario

Table of Contents

Abstract…….....5

Introduction……...7

Chapter 1……...9

1 BIG DATA AND CLIMATE CHANGE…….
1.1 An international need for Climate Action……..……....9
1.2 Climate litigation: some examples of the failure of national executives and legislatures in tackling climate crisis……..12

1.2.1 The Netherlands, *Urgenda*……..13

1.2.2 Ireland, Friends of the Irish Environment (FIE)…….…15
1.2.3 Germany, *Climate Protection Act* case……...17
1.2.4 France, *Grande-Synthe* case……...18
1.3 Adapting environmental law to address individual behaviour as opposed to the one of industries as larger sources of pollution…….20

1.3.1 Informational Regulation and Norm Management - some approaches for regulating environmentally significant individual behaviours……...23
1.4 A universal demand for responsible production practices and the public benefit corporation (PBC)……..26
1.4.1 Greenwashing" or "fairwashing"- when organizations exploit Voluntary Standards using labels certifying their fake adherence to environmental standards……...27
1.4.2 A need for homogenization of Standard and Certification Systems…….29
1.5 Blockchain- a possible tool for countering information asymmetry and guarantee corporate social and environmental responsibility?.....31

Chapter 2……....35

2 SMART GRIDS……..
2.1 A way to enable environmentally sensitive electricity distribution and consumption practices……..35

2.2 The role of the Internet of Things in the smart grid evolution…….....38

2.3 Some examples of inherent initiatives……..38
2.3.1 Radio frequency identification (RFID) technology……..…..38
2.3.2 Ambient Orb - a technology to aid energy conservation……41
2.3.3 PlanetWatch……....42

Chapter 3 47
3 BIG DATA AND PRIVACY ISSUES…….
3.1 Privacy injuries of the Information Age - Negative externalities and the *"tragedy of the commons"*……..……47
3.2 Some existing and proposed limits on the collection or use of personal information related to RFID technology and smart grids (privacy harms)……..….50
3.3 The Naperville Case and its implications……55
3.4 Methods of protecting data and approaches to protect privacy in Smart Grids……..58
3.5 Is it possible to find a balance between regulatory benefits- such as those of smart grids – and privacy protection?.....65

Chapter 4……69
4 PREVAILING APPROACHES TO PRIVACY POLICIES……..
4.1 Basic privacy principles- the FIPPs, the GPDR and AMIs technologies…….69
4.2 Federal Privacy Law- The Fourth Amendment and the third-party doctrine……...76
4.3 Additional privacy protections beyond general privacy principles and federal law…84
4.3.1 How strong privacy laws on smart meters can lead to an increase in smart meters installation- Texas's *Utility Code*……85
4.3.2 The "*opt-out*" policy and data privacy rules- California and Colorado…….88
4.4 Other practices governments have developed both in Europe and in North America to protect privacy with respect to smart-meter or digital-electricity technology……92

Conclusion……..97
RIASSUNTO IN ITALIANO……99
Bibliography……..…108

Abstract

As stated by the UN, Climate Change is the defining issue of our time, and requires nations to take action and cooperate according to a universal demand for responsible production practices. Another defining issue of our time is the Big Data era we are living in. These are two matter of fact situations that would be at the basis of this dissertation, which will illustrate how Big Data could play an essential role in developing strategies to mitigate climate change.

A focus will be made on smart meters and companies which were able to implement new technologies to espouse the climate change cause. However, data collection mostly entails privacy concerns, creating a permanent struggle between the need to enhance technologic innovation and protect privacy as a fundamental human right. Methods and approaches to guarantee that consumers' privacy is respected in smart grids will be analysed. Moreover, we will underline the need for policymakers to understand both the potential environmental benefits offered by access to personal environmental information and their associated privacy costs, finding out new ways and reforms through which these two apparently contrasting realities could meet.

Introduction

To date, 192 nations have adopted the United Nations Framework Convention on Climate Change (UNFCCC) goal, aiming at stabilizing greenhouse gas concentrations in the atmosphere.
Relying on current science, many policymakers worldwide advocate no more than a 2°C rise in long-term global temperature.
Actions aiming at stabilizing atmospheric greenhouse gas concentrations are needed to achieve that goal, which in turn would require a reduction in annual greenhouse gas global emissions of 50% to 80% below 1990 levels by 2050, according to recent studies.
The technological implications and challenges of meeting such a goal are considerable.

The following thesis work intends to delve into Big Data world, demonstrating how new technologies could help mitigate climate change.
The first chapter will be an introductive one and will therefore provide a general framework of current environmental law.
Four court cases will be taken as examples to remark how courts across the globe are increasingly calling on the individual responsibility of states and private companies to intensify efforts towards the collective pursuit of a more sustainable future.
These recent cases highlight the pivotal importance of intergenerational climate justice for attaching legal responsibility to actors who fail to play their part in mitigating climate change.
However, besides private companies, it is also fundamental for individuals to take concrete action against climate change too. For this reason, some approaches for regulating environmentally significant individual behaviours will be presented as well.
The second chapter of this work will be devoted to *Smart Grids* - electricity networks that have profoundly changed the way energy is generated, distributed, and consumed.
Despite smart grids help save a significant amount of energy and resources, they also allow to gather an immense quantity of information that can be handled by various actors, thus letting new privacy related challenges arise.
Being data circulating in the grid highly sensitive, and because of the high frequency and density of these data transactions, traditional means for privacy regulations enforcement often proved insufficient and inadequate.
The third chapter intends therefore to discuss some privacy harms that are related to smart grids and Radio frequency identification technology.

Special attention will be given to the Naperville Case. Indeed, while some citizens are given the opportunity to decide whether to install smart meters or not, Naperville's residents cannot opt out of the smart-meter program.

That was the reason why concerned citizens sued the city of Naperville, claiming that an invasion of privacy under the Illinois Constitution and an unreasonable search under the Fourth Amendment were simultaneously occurring.

This case was relevant for leading to a reflection on the importance of guaranteeing a government search of customer's electricity data is authorized and perceived as such by citizens.

Otherwise, individuals would end up opposing smart grids and similar technologies, thus hindering technological innovation and their potential benefits for the environment.

Finally, the fourth chapter will analyse some prominent privacy policies, with a focus on the Fair Information Practice Principles (FIPPs) and the European General Data Protection Regulation (GDPR).

Both the FIPPs and GDPR provide a general framework for privacy in the digital age.

Nonetheless, the need to envisage more specific clauses to be added to these general privacy principles will be remarked, in light of all the issues posed by electricity customer data in the context of AMIs.

For this purpose, after an analysis of The Fourth Amendment and the third party doctrine, the last part of the chapter will be dedicated to the effort some governments have undertaken to implement their own privacy policies in relation to smart-meter or digital-electricity technology.

Although it is proving difficult to achieve, the need to find a balance between consumers privacy and AMI technologies underlies this work.

There is no unique solution or pathway to achieving large reductions in greenhouse gas emissions.

What is sure is that, as all models demonstrate, dramatic changes in the energy system will be required. Energy is the dominant contributor to climate change, and we need to consider smart grids and smart meters as an ally not as a weapon that could jeopardise our right to privacy.

We all agree on that fact that privacy laws must be enforced.

However, we will explore the possibility to set a *technical* enforcement to ensure compliance with privacy regulations.

Chapter 1

Big Data and Climate Change

This dissertation aims to demonstrate that Big Data can play an important role in accelerating climate action, sustaining climate change projects. In order to do so, after a brief introduction focused on the international need to engage in climate action, Chapter 1 will illustrate the facts of four exemplary cases in which governments and national parliaments proved unable to take effective measures to tackle climate crisis. Thirdly, this Chapter will demonstrate how personal environmental information produced by technology could improve the regulation of environmentally significant individual behaviours.

The contrast between the demand of environmental responsible production practices for companies and the spread of "*greenwashing*" or *"fairwashing"*, will be analyzed too.

Chapter 1 will conclude claiming the need to implement universally valid standard and certification systems and proposing an open question, namely: "Can the blockchain technology be a possible tool for countering information asymmetry and guarantee corporate social and environmental responsibility?"

1.1 An international need for Climate Action

Nowadays, it is common knowledge that if current trends continue, future global emissions of greenhouse gases will grow significantly and, as a consequence, global warming will seriously jeopardize agriculture, water supplies, human health, and settlements especially in coastal areas which are more likely to be affected by rises in sea level and storms[2].

On 12 December 2015, 195 State Parties under the United Nations Framework Convention on Climate Change adopted the Paris Agreement. This legally binding international agreement on climate change arises from a common cause that brought countries together, namely limiting global warming and keeping global average temperature increases to 1.5 degrees Celsius.[3]

[2] Rubin, E S. (2010). *Innovation and Climate Change.* Source: NRC. Carnegie Mellon University. pg. 335.
[3] Rimmer, M. (2018). *Intellectual property and clean energy: the Paris Agreement and climate justice.* Singapore Springer Singapore. pg. 116.
Brutti, N. (2022). *Le regole dell'informazione ambientale, tra pubblico e privato.* pg. 24.

Despite being a "significant step forward in international climate politics"[4], the implementation of these long-term temperature goal requires some adaptation and mitigation techniques.

This work will delve into the use of existing technologies for improving resilience to climate change and reducing greenhouse gas emissions, even if implementation strategies for the Paris Agreement are valid also for many other fields such as finance or capacity building.

2020 was the deadline for submission of national plans for climate action which are known as nationally determined contributions (NDCs). National governments have therefore huge responsibilities and duties to take action to reduce their countries' greenhouse gas emissions. Therefore, since climate change entails long-term implications, reaching the Paris Agreement goals responds to the moral duty to protect future generations.

As a matter of fact, laws and policies should not only promote a rational, sustainable, and safe management of natural resources to contribute to the protection of peoples; they should also consider "the needs of future generations in determining the rate of use of natural resources, working to fulfil a community or country's duty to avoid wasteful use of natural resources"[5].

According to this principle, regulatory government policies are needed to limit greenhouse gas emissions and foster technological innovation. However, since intergenerational justice issues are best handled with the participation of "concerned" citizens[6], both the private sector and individuals in general should be taken into account in this process.

In other words, governments have a fundamental role in fostering innovations to combat climate change, but private companies have a critical role too. Indeed, they need to find out and retain the brightest minds to address environmental challenges and "invent the opportunities for mitigating global climate change"[7].

However, the "unprecedented and inter-generational nature of climate change" calls for the involvement of civil society bodies and individuals to "realign consumption, reshape infrastructure investment and, more broadly, influence public policy"[8].

It is important for laws and policies to guarantee access to adequate information and encourage citizens to play an active role in decision-making processes affecting their lives and well-being[9].

[4] Rimmer, M. Cit.
[5] Cordonier Segger, M-C, Rana, R. et al. (2008). *Selecting Best Policies and Law for Future Generations: legal working paper and worked examples*, World Future Council CISDL, Montreal, Canada. pg. 10.
[6] Cordonier Segger, M-C, Rana, R. et al. Cit. pg.14.
[7] Rubin, E S. Cit. pg. 348.
[8] Rimmer, M. Cit.pg.376.
[9] Cordonier Segger, M-C, Rana, R. et al. Cit.

Accordingly, it is worthy to note that a convention claiming these principles was already signed on 25 June 1998 in the Danish city of Aarhus.

The Aarhus Convention granted a number of public environmental rights to individuals and their associations. In particular, it provides the "right to receive environmental information held by public authorities", "the right to participate in environmental decision-making" and the right to have "access to justice" [10].

An important link between environmental protection and the right to information and democratic participation was created thanks to this convention[11]. According to the Aarhus Convention, applicants can obtain information on the state of the environment, on policies or on the state of human health and safety- whether this can be affected by the state of the environment- within one month and without having to explain the reason why they require it[12].

The right to have access to this kind of information, is a key element of modern constitutions and is destined to influence every decision-making process in democratic societies[13].

Nowadays, some scholars affirm that since technological advances can make environmental protection more data-driven and analytically rigorous, the spreading of environmental data could increase "transparency" and weaken governmental control over decision making[14].

As a matter of fact, when citizens, environmental groups, or the media, find out exemplary environmental management systems in other countries, they have a reason to demonstrate disappointment if they perceive their government is not doing as well as them.

For instance, when the 2001 World Economic Forum Environmental Sustainability Index ranked Belgium seventy-ninth, people started complaining and protesting in Brussels[15]. Environmental groups, the media, and opposition politicians pressed the government to explain why the nation had such poor control on pollution and a **"**major rethinking of Belgium's environmental approach began"[16].

With the adoption of this data-driven environmental management system bad acts and poor environmental policies could become almost impossible to hide.

---

[10] European Commission. *Aarhus Convention* : https://ec.europa.eu/environment/aarhus/ [10/07/2022]

[11] Brutti, N. (2005). *Il diritto all'informazione ambientale*, *Profili comparatistici*. Torino, Giappichelli pg.36.

[12] European Commission. Cit.

[13] Brutti, N. (2005). Cit. pp. 17-18.

[14] Esty, D C. (2003). *Environmental Protection in the Information Age*. pg. 167.

[15] Esty, D C. Cit. pg.168.

[16] Ibid

As data become easier to analyse and spread, and less costly to acquire and use, environmental problems will become even more effortlessly identifiable and fixable[17].

Even though a uniform definition is lacking[18], the term "Big Data" refers to the management of large volumes of data which can be used in predictive modelling[19], machine learning or other advanced analytics projects.

Passively collected digital data can "enhance the monitoring of climate-related threats and vulnerabilities and can provide real-time awareness and feedback to decision makers and emergency services"[20].

In conclusion, Big Data and new technologies can "revivify democracy" through individual and community participation in the processes of developing standards or strategic choices in environmental matters[21].

For these reasons, climate action and technological progress are not opposing concepts. On the contrary, climate action must guide and cooperate with technological progress.[22]

1.2 Climate litigation: some examples of the failure of national executives and legislatures in tackling climate crisis

To date, many European governments have proved unable to ensure effective policy design and implementation to mitigate climate crisis. The consistent failure of "politics" in the international, European, and national, or even regional and local context, pushed citizens and civil society actors to pursue institutions and companies through "counter-majoritarian instruments"[23], most notably via climate litigation.

"Climate litigation is an increasingly common and accessible area of environmental law"[24].

---

[17] Esty, D C. Cit. pg. 119.

[18] Ford, D J. et al. (2016). *Big Data has Big Potential for Applications to Climate Change Adaptation,* in Proceedings of the National Academy of Sciences, 113:39 NNAS 10729. pg.1.

[19] Brutti, N. (2022). Cit. pp. 34-35.

[20] Ford, D J. et al., Cit. pg. 3.

[21] Brutti, N. (2005). Cit.

[22] Brutti, N. (2022). Cit. pg. 189.

[23] Eckes, C. (2022). *Tackling the Climate Crisis with Counter-majoritarian Instruments: Judges Between Political Paralysis, Science, and International Law.* European Papers Vol. 6, 2021, No 3. pg. 1307.

[24] Mishra, S. (2022) *The Rise of Climate Litigation.* Harvard Law School Forum on Corporate Governance. Institutional Shareholder Services, Inc.: https://corpgov.law.harvard.edu/2022/03/03/the-rise-of-climate-litigation/

Through this legal procedure, countries and public corporations are obliged to justify and provide proof of their climate mitigation efforts and contributions to the climate change cause[25]. The reasons of the diffusion of climate litigation can be found on the fact that courts have an increasingly active role both in quantity and quality[26]. However, despite this increase in seeking justice through climate litigation, it is common belief that countries will take their environmental responsibilities seriously and undertake more concrete actions "as the negative impacts of climate change increasingly affect their lives and livelihoods"[27].

This section will examine four cases that brought out new features and thoughts about the role of judges in climate litigation. All the four cases (*Urgenda, Friends of the Irish Environment* case*, Grande-Synthe* case and *German Climate Protection Act* case) dealt with countries being required by national courts to reduce their overall national emissions respectively in the Netherlands, Ireland, France and Germany[28].

1.2.1 The Netherlands, *Urgenda*

Dutch greenhouse gas emissions had to be reduced by 25% compared to 1990 levels by the end of 2020. This was ruled by The Hague District Court in 2015 in the case of the *Urgenda Foundation*.[29]

Apart from representing a victory in fighting climate change, this judgment was regarded as a "milestone in public interest litigation" in the Netherlands and worldwide[30]. It was indeed the first time a court had ordered a government to "limit greenhouse gas emissions for reasons other than statutory mandates"[31].

In 2017, greenhouse gas emissions were reduced by 13% over 1990 levels, although this percentage did not take account of carbon dioxide emissions, which on the contrary, increased by approximately

[25] Ibid
[26] Eckes, C. Cit. pg.1317.
[27] Eckes, C. Cit. pg.1307.
[28] Eckes, C. Cit. pg.1308.
[29]Government of the Netherlands. *Climate Policy*: https://www.government.nl/topics/climate-change/climate-policy [11/07/2022]
Backes, C.W., van der Veen, G.A. (2020). *Urgenda: the final judgment of the Dutch Supreme Court*. J. Eur. Environ. Plann. Law 17(3), pg. 308.
[30] Ibid.
[31] Sabin Center for Climate Change Law. (2020). U.S. Litigation Chart made in collaboration with Arnold & Porter Kaye Scholer LLP**.** *Urgenda Foundation v. State of the Netherlands.* http://climatecasechart.com/non-us-case/urgenda-foundation-v-kingdom-of-the-netherlands/
[11/07/2022]

2 megatons[32]. It is for this reason that The Dutch government was sued by the *Urgenda Foundation*- a Dutch environmental group, and 900 Dutch citizens.

The Hague District Court claimed the Netherlands as a State had expressly avoided its responsibilities, "making unreasonable downwards adjustments to earlier reduction targets"[33] and consequently, justifying inaction in face of an existential threat[34].

Invoking the European Court of Human Rights' (ECHR) case law, the Supreme Court judged that appropriate measures must be adopted when there is evidence of a real threat to the lives and well-being of individuals[35]. This applies to environmental risks affecting people and which may occur both in the long term and in the short term[36].

As previously stated, another aspect the court dealt with is the kind of responsibility the Netherlands have in the global context. In other words, a country cannot duck its responsibility hiding behind the misconception that its emissions are relatively limited compared with the rest of the world, and that reducing them would not make a great difference on a global scale[37]. The concept of a "fair share of the global responsibility"[38], needs to be kept in mind since it will be a benchmark notion for all the other cases that will be analysed in this Chapter. Precisely in this perspective, the Dutch government had to guarantee it would still "contribute a fair share to the reduction of greenhouse gases if the reduction in 2020 were as little as 20 percent and would be accelerated after 2020"[39].

In 2020, Dutch greenhouse gas emissions were 25.5 percent below the level of 1990, meaning that the "Urgenda goal" was reached[40]. From 2015 to 2020, emissions by coal-fired power stations were reduced by 80 percent[41]. Moreover, since 2020 was a relatively warm year, less natural gas was needed for heating than in 2019 and because of the coronavirus pandemic, road transport emissions were 15 percent lower than in 2019[42].

Given that in the Netherlands there is no specific binding legislative climate act establishing reduction targets for protecting the environment, the State's obligation to reduce emissions found its bases on the rights to life and to private and family life under articles 2 and 8 of the European Convention on

---

[32] Ibid.
[33] Backes, C.W., van der Veen, G.A. Cit. pg. 320.
[34] Eckes, C. Cit. pg. 1310.
[35]Backes, C.W., van der Veen, G.A. Cit. pg.309.
[36] Ibid.
[37] Ibid.
[38] Ibid.
[39] Ibid.
[40] Facts that matter. CBS (2022) *Urgenda reduction target for GHG emissions achieved in 2020:* https://www.cbs.nl/en-gb/news/2022/06/urgenda-reduction-target-for-ghg-emissions-achieved-in-2020
[11/07/2022]
[41] Ibid
[42] Ibid.

Human Rights (ECHR)[43]. Based on international human rights obligations and national tort law, the decision of the Dutch Supreme Court marks an historic development in international jurisprudence on climate change because it demonstrated that a domestic court could enforce compliance with international treaties against a national government[44].

1.2.2 Ireland, Friends of the Irish Environment (FIE)

The 2015 *Climate Action and Low Carbon Development Act,* with which Ireland manifested its commitment to pursue the "transition to a low carbon, climate resilient and environmentally sustainable economy by 2050", required the government to publish a National Mitigation Plan.
This plan, published in 2017, had to indicate the measures Irish government intended to take to reach its environmental goals. However, it turned out to be "wholly inadequate"[45].
Climate Action and Low Carbon Development Act established the need for Ireland to achieve "an aggregate reduction in carbon emissions of at least 80 percent in some sectors and zero net emissions in others"[46] by 2050. Nevertheless, the National Mitigation Plan let emissions increase and consequently, a national law required the government to specify how it was planning to achieve its reduction goal.
Friends of the Irish Environment (FIE), a prominent advocacy group, sought judicial review of the Plan, claiming that the government's approval of the National Mitigation Plan violated the Climate Action and Low Carbon Development Act[47]. Moreover, they argued that a violation of fundamental rights such as the right to life and the right to private and family life[48] was occurring too.
The case was argued before the Supreme Court on January 22, 2019. The court refused the argument concerning a violation of Ireland's Constitution Rights and put off the decision less than a year later.[49]
FIE appealed the decision to the Court of Appeal on November 22, 2019, and on February 13, 2020, the Supreme Court agreed to hear the case, recognizing there was urgency concerning "the adoption

---

[43] Eckes, C. Cit. pg.1313.
[44] Shannon, N. de Wit, E. (2019) *Urgenda Foundation v Netherlands: Historic climate change decision upheld* https://www.nortonrosefulbright.com/en-au/knowledge/publications/45dc4f83/urgenda-foundation-v-netherlands-historic-climate-change-decision-upheld
[11/07/2022]
[45] Alston, P. and Adelmant, V and Blainey, M. (2021). *Courts, Climate Action and Human Rights: Lessons from the Friends of the Irish Environment v. Ireland Case.* Litigating the Climate Emergency: How Human Rights, Courts and Legal Mobilization Can Bolster Climate Action (Cambridge University Press). pg.2.
[46] Eckes, C. Cit. pg. 1310.
[47] Sabin Center for Climate Change Law. Cit.
[48] Sabin Center for Climate Change Law. Cit.
Alston, P. and Adelmant, V and Blainey, M. Cit. pg.2.
[49] Ibid.

of remedial environmental measures"[50]. On July 31, 2020, the National Mitigation Plan was found to be ultra vires and was quashed, specifying that "a compliant plan must be sufficiently specific as to policy over the whole period to 2050"[51].

Inspired by the Dutch judgment *Urgenda*[52], FIE was not entirely satisfied with the final ruling, since they hoped the court would recognize the government "had a duty, arising from international human rights and constitutional rights, to do more to reduce greenhouse gas emissions"[53].

However, this ruling is to be regarded as a pioneering one, at least as far as future approaches to such issues are concerned[54]. Indeed, this case demonstrated that citizens "need to be able to hold their government to account" when they notice it is failing to live up to its duties[55].

Furthermore, the Court's judgment remarked the importance of "developing a trajectory" focusing "on overall emissions rather than emission targets at a given moment"[56]. This point reminds the Climate Protection Act case, which made the adoption of a more global approach possible.

As a matter of fact, nowadays, "while annual emission limits for the period 2021 to 2030 will guide Ireland towards the 2030 target, the main binding target will be for cumulative emissions"[57].

Ireland will have to achieve a 30 percent greenhouse gas emissions reduction by 2030, relative to 2005 levels[58] and the Government also supports the adoption of a net zero target by 2050 at European level.

The Climate Action Plan commits to evaluating in detail the changes that need to be made to reach this target[59].

In conclusion, *Friends of the Irish Environment v. Government of Ireland & Ors* (hereafter FIE) is another landmark case, highlighting the urgency to opt for "strategic use of regional and international mechanisms in addition to domestic courts for climate cases"[60], allowing to outline vague measures

[50] Sabin Center for Climate Change Law. Cit.
[51] Ibid.
Alston, P. and Adelmant, V and Blainey, M. Cit. pg.2.
[52] Alston, P. and Adelmant, V and Blainey, M. Cit. pg.2.
[53] Ibid.
[54] Alston, P. and Adelmant, V and Blainey, M. Cit. pg.3.
[55] Eckes, C. Cit. pg.1311.
[56] Eckes, C. Cit. pg.1314.
[57] Government of Ireland. (2019). *Climate Action Plan to Tackle Climate Breakdown.* pg.22. https://webcache.googleusercontent.com/search?q=cache:qh1Qoa1JCToJ:https://assets.gov.ie/10206/d042e174c1654c6ca14f39242fb07d22.pdf&cd=3&hl=it&ct=clnk&gl=it
[12/07/2022].
[58] Government of Ireland. Cit. pg.19.
[59] Government of Ireland. Cit. pg.23.
[60] Alston, P. and Adelmant, V and Blainey, M. Cit. pg.1.

or deferred actions in the hope that "future technologies would come to the rescue", helping envisage increased greenhouse gas emissions[61].

1.2.3 Germany, *Climate Protection Act* case

Germany's Federal Climate Change Act (CCA) was adopted in 2019 and reformed in 2021. This institutional reform was formulated to increase the nation's future capacity to achieve its climate goals. As a matter of fact, "Germany missed its national emission reduction target in 2005" and barely achieved the one due by 2020- likely only because of the preventive measures put in place to control COVID-19 transmission[62].

The Federal Climate Change Act aims to ensure achievement and compliance with national and the Paris Agreement climate targets[63]. It is to this end that the CCA legislated a "policy adjustment mechanism and an independent expert advisory body, proving to be the most important institutional reform in the history of German climate governance"[64].

However, Germany had to amend the Climate Protection Act after its Constitutional Court ruled it unconstitutional in parts. Indeed, in March 2021, the German Constitutional Court (GCC) held that "the national Climate Protection Act violated fundamental rights protected under the German Constitution"[65]. The GCC fully explained that the legislature failed to set sufficient provisions for emission cuts beyond 2030, thus "violating the constitutionally protected fundamental rights of the complainants by irreversibly offloading major emission reduction burdens into the future, namely to after 2030"[66].

Another interesting aspect related to this case is GCC's approach to science. In particular, the GCC started from the temperature goal stipulated in the Climate Change Act to determine the State's cumulative carbon emission target. This temperature target was then turned into a national carbon budget, relying on the advice of the expert council for environmental questions, which in turn had built their calculations upon "the work of the Intergovernmental Panel on Climate Change (IPCC)[67], establishing a global carbon budget"[68].

---

[61] Ibid.
[62] Flachsland, C and Levi, S. (2021). *Germany's Federal Climate Change Act.* Environmental Politics, 30:sup1, pp. S127-128.
[63] Ibid.
[64] Ibid.
[65] Eckes, C. Cit. pg.1311.
[66] Eckes, C. Cit. pg. 1314.
[67] The Intergovernmental Panel on Climate Change (IPCC) is the United Nations body for assessing the science related to climate change. The IPCC prepares comprehensive Assessment Reports about the state of scientific, technical and socio-economic knowledge on climate change, its impacts and future risks, and options for reducing the rate at which climate change is taking place. https://www.ipcc.ch/
[68] Ibid.

This new shift of the focus to total carbon budgets is fundamental since emissions have a long-term impact on the climate thus, it is the total amount of emissions that will determine our climate, not the reduction percentage registered each year[69].

The case is also interesting because of the importance it gives to intergenerational justice and responsibilities. Ruling that the legislature must follow a carbon budget approach to limit warming to well below 2°C, or even to 1.5°C, the Court determined that the budget between current and future generations was not proportionally distributed[70]. Germany has the duty to protect the interests of future generations. It was indeed claimed that one generation cannot use up "large portions of the CO2 budget while bearing a relatively minor share of the reduction effort, if this would involve leaving subsequent generations with a drastic reduction burden and expose their lives to serious losses of freedom"[71].

The court ordered the German legislator to set clear provisions for reduction targets from 2031 onward by the end of 2022[72]. With regards to this decision, the federal lawmakers passed an amended Climate Change Act, with which Germany shall reduce its greenhouse gas emissions:

- by 65 percent compared to 1990 by 2030 (instead of currently 55 percent)
- by 88 percent compared to 1990 by 2040 (no prior goal)
- achieve climate neutrality by 2045 (instead of currently by 2050)[73]

1.2.4 France, *Grande-Synthe* case

On November 19th, 2021, the municipality of Grande-Synthe- located in northern France- together with several associations, asked the *Conseil d'État,* namely the highest Administrative Court in France, to undo the Government's refusal to undertake additional measures to reach the Paris Agreement greenhouse gas emissions' reduction target[74].

---

[69] Ibid.
[70] Sabin Center for Climate Change Law. Cit.
[71] Sabin Center for Climate Change Law. Cit.
[72] Ibid.
[73] Sabin Center for Climate Change Law. Cit.
Burianski M., Parise Kuhnle F. (2021). *Reshaping Climate Change Law: The German Federal Constitutional Court Orders the German Legislator to Set Clear CO2 Emission Reduction Goals Beyond 2030*:
https://www.whitecase.com/publications/alert/reshaping-climate-change-law
[14/07/2022]
[74] Conseil d'État. (2021). *Greenhouse gas emissions: the Conseil d'État annuls the Government's refusal to take additional measures and orders it to take these measures before 31 March 2022*
https://www.conseil-etat.fr/en/news/greenhouse-gas-emissions-the-conseil-d-etat-annuls-the-government-s-refusal-to-take-additional-measures-and-orders-it-to-take-these-measures-befor
[14/07/2022]

In July 2021, the *Conseil d'État* held that the measures French Government was adopting at that moment were inadequate. As a matter of fact, they would not make it possible to achieve the national law climate targets of reducing greenhouse gas emissions by 40 percent by 2030[75].

To be precise, the trajectory drawn up by the Government covered four periods (2015-2018, 2019-2023, 2024-2028 and 2029-2033) and in each of them four respective reduction targets could be identified[76].

Even though a reduction in greenhouse gas emissions was measured in 2019, the *Conseil d'État* considered it was too limited compared to the reduction targets for the previous period (1.9 percent per year) and to the targets established for the following one (3 percent per year).

Furthermore, even the significant reduction data show for 2020 were judged insufficient, given the health crisis and lockdowns due to COVID-19 pandemics, characterising that year[77]. This statement is related to the February 2021 report of France's High Council on Climate (HCC), which considered the 2020 reduction "transitory" and "at risk of upturns"[78]. The HCC released its annual report the day before the ruling of the *Conseil d'État*, requiring France to "double its reduction efforts from 2021"[79].

Another point the *Conseil d'État* examined is the European Climate Law, the legally binding target of net zero greenhouse gas emissions by 2050 adopted by the European Parliament and the Council, which dramatically raises Europe's (and consequently France's) target for reducing greenhouse gas emissions from 40 percent to 55 percent compared to their 1990 level[80].

With the decision of the *Conseil d'État*, French Government was given nine months to take appropriate measures to reach emissions' levels complying with the Paris Agreement.[81]

Thanks to the *Grande-Synthe* case there is now a "clear judicial precedent in France to challenge climate inaction, set by the highest administrative court of the land"[82].

Even if no concrete measures were prescribed to the government, the *Conseil d'État* put pressure on French government asking for the implementation of "new, sufficient measures and by setting a clear deadline for these additional measures"[83]. For this reason, this case can be regarded as another

[75] Eckes, C. Cit. pp.1311-1312.
Conseil d'État. Cit.
[76] Conseil d'État. Cit.
[77] Arriba-Sellier, N. (2021). *The Grande Synthe Saga Continues: A Pyrrhic victory for climate litigation?* VerfBlog. pg.1.
[78] Ibid.
Conseil d'État. Cit.
[79] Arriba-Sellier, N. Cit. pg.1.
[80] Arriba-Sellier, N. Cit. pg.2.
Conseil d'État. Cit.
[81] Eckes, C. Cit. pg.1312.
[82] Arriba-Sellier, N. Cit. pg.2.
[83] Ibid.

relevant contribution to the growing international body of case law dealing with the protection of future generations' environmental rights[84].

In conclusion, the four plaintiffs and the courts' approaches that have just been analysed are considerably different[85].
The difference between them lies in national circumstances, such as "whether national climate legislation exists; whether the constitution contains relevant state policy objectives […] and how duties under national tort law are formulated"[86]. Nevertheless, a common feature to all cases is international law and science background, e.g., the Paris Agreement and the IPCC's work that are often invoked.[87]
The victory of these climate litigants is partly due to the "use of non-binding international norms together with overwhelming science to give meaning to legally enforceable national or international obligations"[88]. Put in other words, these cases show how States have refrained from making more concrete international legal commitments concerning emission's reduction targets that could directly be enforced before courts and demonstrate on the contrary that climate litigation is an efficient counter-majoritarian instrument in democracies to make up for this lack[89].

1.3 Adapting environmental law to address individual behaviour as opposed to the one of industries as larger sources of pollution

"The Congress recognizes that each person should enjoy a healthful environment and that each person has a responsibility to contribute to the preservation and enhancement of the environment."[90] That is the second, in a series of three articles of the *Congressional declaration of national environmental policy*, which can be found in The National Environmental Policy Act of 1969.

[84] Eckes, C. Cit. pg.1312.
[85] Eckes, C. Cit. pg.1315.
[86] Ibid.
[87] Ibid.
[88] Eckes, C. Cit. pg.1315.
[89] Ibid.
[90] Legal Information Institute: Open access to law since 1992. *42 U.S. Code § 4331 - Congressional declaration of national environmental policy.*
https://www.law.cornell.edu/uscode/text/42/4331#:~:text=The%20Congress%20recognizes%20that%20each,I%2C%20%C2%A7%20101%2C%20Jan.
[15/07/2022]

The need to make individuals understand that their activities not only have an impact on the environment, but sometimes can be equal to or even greater than those arising from industrial sources[91], is becoming increasingly urgent.

Indeed, one of the main factors preventing individuals to behave more environmentally responsibly is the misperception they have about their impact on the environment. Generally, people think their "individual contributions to environmental problems are small and, therefore, inconsequential"[92]. This firm belief of not being directly responsible for environmental degradation makes them avoid any behaviour change they may consider costly or inconvenient[93].

On the contrary, personal consumption is a significant source of environmental issues[94]. For instance, in 1998 in the United States thirty-eight million cars were produced and simultaneously the number of people per car diminished by almost 80 percent over the previous fifty years [95].

Individuals contribute to pollution in amounts that are often invisible when released, but inflict harms that are usually chronic, and their impact becomes serious only when these small sources are aggregated over time or with the contributions of others[96]. As a matter of fact, nowadays the cumulative impact of small-source emissions represents, in most cases, the cause of persistent pollution problems in many fields[97].

Quoting Alan Thein During:

> In the aggregate, global consumption achieved a level that is almost historically inconceivable: measured in constant dollars, the world's people have consumed as many goods and services since 1950 as all previous generations put together[98].

[91] Babcock, H M. (2009). *Assuming Personal Responsibility for Improving the Environment: Moving Toward a New Environmental Norm*. Georgetown Law Faculty Publications and Other Works. pg.121.
[92] Babcock, H M. Cit. pg.119.
[93] Ibid.
[94] Babcock, H M. Cit.pg.122.
[95] Ibid.
[96] Fischer Kuh, K. (2012). *Personal Environmental Information: The Promise and Perils of the Emerging Capacity to Identify Individual Environmental Harms*, 65 VAND. L. REV. 1565, pg. 1575.
Flachsland, C and Levi, S. (2021). *Germany's Federal Climate Change Act.* Environmental Politics, 30:supl. pg.1575.
Esty, D C. Cit. pg.196.
Babcock, H M. Cit.pg.120.
[97] Esty, D C. Cit. pg.196.
Babcock, H M. Cit.pg.120.
[98] Durning, Alan Thein (1992), How Much is Enough?, London: Earthscan. pg.29.

William Ruckelshaus, the first Administrator of the US Environmental Protection Agency (EPA)[99] from 1970 to 1973, acknowledged that nowadays the most significant threats to our environment seem not to be deriving from major industrial sites, but from "the habits of ordinary Americans".
This statement can be applied to every single individual's habit, since "each of us pollutes when we drive our cars, fertilize and mow our yards, pour household chemicals on the ground or down the drain, and engage in myriad other common activities"[100].
Moreover, as stated in the first paragraph of this work, "this individualistic […] behaviour can even jeopardise the interests of future generations"[101]. Thus, even if some existing environmental policies often underestimate the importance of small harms, this logic for ignoring them is no longer viable "as the cost of tracking and internalizing [small harms] drops"[102].
Furthermore, the regulatory target represented by individuals is notably different from the archetypal regulatory target employed in environmental law, namely the polluting factory.
As a matter of fact, "individuals are more numerous and more widely dispersed"[103] and it is more likely they will react differently to regulatory intervention and government efforts to control their behaviours, by arguing against government intrusion[104].
It is for this reason that environmental law and policy should be adapted to better and more directly address individual behaviour as opposed to the behaviour of large, industrial sources of pollution[105].
In this context, Lawrence Lessig's taxonomy is a useful tool for understanding how a modern regulatory regime can try to regulate behaviour[106].
Lawrence Lessig is an American jurist and Professor of law at Harvard Law School, founder of Creative Commons, a non-profit organization aiming at expanding the availability and legal share of copyright works[107], who distinguishes four constraints to regulate behaviour. These constraints are law (or mandates), norms, the market, and architecture[108].
While laws or mandates impose requirements on behaviour and provide sanctions if those requirements are not met, norms aims at regulating behaviour both through expectations the community impose (external, or social norms) or through individuals' expectancies (internal, or

[99] The EPA is an independent executive agency of the United States federal government created by President Richard Nixon on July 9, 1970, for the protection of the environment. The EPA is led by its administrator, who is chosen by the president and approved by the Senate; the current administrator is Michael S. Regan. https://www.epa.gov/
[100] Babcock, H M. Cit. pg.120.
[101] Brutti, N. (2022). Cit. pg.2.
[102] Esty, D C. Cit. pg.196.
[103] Fischer Kuh, K. Cit. pg.1575.
[104] Ibid.
[105] Ibid.
[106] Fischer Kuh, K. Cit. pg.1576.
[107] Rimmer, M. Cit. pg.526.
[108] Fischer Kuh, K. Cit. pg.1576.

personal norms). As far as architecture is concerned, this term indicates "features of the world [that] restrict and enable in a way that directs or affects behaviour and includes, for example, the built environment"[109].

Any of these four modalities of regulation can help governments to influence individual behaviours. This can be done directly (through mandates) or indirectly (by regulating norms, the market, or architecture).

The next part of this paragraph will analyse the regulation of environmentally significant individual behaviours.

Since people are more likely to react to what they perceive as directly impacting them or their descendants, "a willingness to act beyond the present might be encouraged by integrating up-to-date information with information about the future"[110].

In doing so, an inter-generational duty should be recognized, accepting costs now with the awareness that if climate action is not progressively taken on a local and global level, future societies will have to face a "physically and politically more precarious existence"[111].

A way to enhance this process is by using personal environmental information generated by advances in technology, such as those environmental information systems referred to as *smart grids*, along with open access to environmental information[112]. The effectiveness of smart grids as tools for achieving climate justice will be discussed in Chapter 2.

1.3.1 Informational Regulation and Norm Management - some approaches for regulating environmentally significant individual behaviours

"Informational regulation and norm management may be the most promising approaches for regulating environmentally significant individual behaviors"[113].

Individuals are prompt to change their behaviours mainly for three reasons: costs imposed on them, internal norms, and external norms. For instance, they may voluntarily cut back environmentally harmful behaviours because of some previously unknown costs (dictated by the market) arising from these behaviours, because they are driven by a personal, moral duty (internal norms), or again because they believe that society expects them to do so (external norms)[114].

[109] Ibid.
[110] Rimmer, M. Cit. pg.378.
[111] Ibid.
[112] Rimmer, M. Cit. pg.379.
[113] Fischer Kuh, K. Cit. pg.1577.
[114] Ibid.

Ann Carlson, a leading scholar of climate change and air pollution law and policy, affirms that while norms may elicit some "cooperative efforts" at first, they may not independently lead to behavioural change[115]. She claims that even if the intensity with which an individual adheres to a social norm is a sign of "her willingness to undertake behaviour that requires effort on her part", the fact of lowering this effort can have a more permanent effect on behaviour than strengthening social norms[116].

Carlson draws this conclusion thanks to her empirical research. Indeed, data showed that "making it easy and convenient to recycle is more important than [creating a] concrete social norm favouring recycling"[117], since people need to be autonomously convinced that they should undertake significant and moral actions.

However, norms can play a role in influencing individual behaviour too. In particular, if there is general consensus about the validity of a norm, and people perceive they could cause harm if they do not respect it, a sense of obligation to conform personal behaviour to the norm may thereby emerge[118].

Technological advance can play an important role in this context. Technology can indeed help develop a communication system spreading information leading individuals and communities to realize that their irresponsible behaviours can be related to environmental harms[119]. In this way, it can "support the activation and development of norms governing specific, concrete individual behaviours"[120].

The form of personal commitment cited above, exists independently of government's decisions but when no monetary benefit arises from the changed behaviour, an incentive to comply with the norm is needed[121]. Such impetus can be provided by the intervention of some organizations or of the government itself.

Carlson believes government's role in this case is limited to encouraging "positive behaviour indirectly", such as publicizing preferred behaviour, laying down penalties, passing laws, and "inculcat[ing] norms of legal compliance by increasing the effort involved in behaving badly"[122].

Nonetheless, the author believes that government is not able to really make people change their behaviour since it is not an "ingroup source" and therefore, as an outgroup, what it wants to convey will be disregarded[123]. As a rule, mandates are not regarded as possible ways to help change

[115] Babcock, H M. Cit.pg.141.
[116] Babcock, H M. Cit.pg.141.
[117] Ibid.
[118] Babcock, H M. Cit.pg.142.
[119] Fischer Kuh, K. Cit. pg.1580.
[120] Ibid.
[121] Fischer Kuh, K. Cit. pg.1580.
[122] Babcock, H M. Cit.pg.147.
[123] Babcock, H M. Cit.pg.150.

environmentally significant individual behaviours because of the costs, administrative challenges, and risk of backlash they impose[124].

Despite not being the major promoter of behavioural change, government can encourage voluntary changes in environmental behaviours through informational regulation. In other words, since technology can enable more ready access to personal environmental information, government could use that information to influence individual significant behaviours.

As a matter of fact, technology can dig up better information, identifying individual behaviours and their associated harms, as well as "reducing the administrative burdens associated with identifying and sanctioning"[125] environmentally unfriendly behaviours.

Moreover, public information campaigns could be organized to educate individuals on potential environmental harms and pave the way for the development of new or more adequate social norms regulating individual environmental behaviours[126]. In doing so, personal environmental behaviours will become more visible and comparable[127]. In this context, an observable and measurable behaviour may be needed for verifying compliance with social norms[128].

Thanks to technological progress "we […] are approaching the day when virtually all emissions will be susceptible to tagging, tracking, and measurement at relatively low cost"[129].

As far as architecture is concerned, technology may also offer the possibility to track the response to changes in infrastructure more easily, "allowing regulators to make adjustments that enhance environmental gains or avoid unintended environmental harms"[130].

Nowadays, smart appliances are connected to "smart meter infrastructure" and can therefore signal peak rates and keep the device on but automatically switch into a reduced electricity usage or a power saving mode[131].

However, product mandates setting minimum standards of energy efficiency could turn out to be a double-edged sword. As a matter of fact, when a product is more energy efficient, individuals may use the product more, reducing or nullifying any potential energy-saving gains, generating what is regarded as the "rebound effect"[132].

[124] Fischer Kuh, K. Cit. pg.1593.
[125] Fischer Kuh, K. Cit. pg.1594.
[126] Fischer Kuh, K. Cit. pg.1580.
[127] Fischer Kuh, K. Cit. pg.1582.
[128] Ibid.
[129] Esty, D C. Cit. pg.157.
[130] Fischer Kuh, K. Cit. pg.1593.
[131] Fischer Kuh, K. Cit. pg.1592.
[132] Fischer Kuh, K. Cit. pg.1593.

Smart meters could offer a solution even in this case, tracking the use of energy of each appliance, and detecting eventual increases in frequency of use, or a rebound effect.
Consequently, better information about environmentally significant behaviours can also be a driving force of architecture reform towards environmental protection[133].
Nevertheless, the fact of allowing all this data to be manipulated and disseminated can lead to "privacy and related intrusion objections"[134]. These issues will be further analysed in Chapter 3.

1.4 A universal demand for responsible production practices and the public benefit corporation (PBC)

Today consumers are increasingly looking for "businesses with socially and environmentally responsible practices"[135].
At the same time, a parallel demand for transparency involves corporations, which are more and more inclined to impose environmentally and socially responsible standards on themselves and their supply chains[136]. Meeting modern consumers demand for more accountability on corporate practices and business choices, has become a priority by now. Thereby, a great number of companies have developed sophisticated environmental programs, and there is a general recognition among business executives of the need "to go beyond mere compliance with regulatory requirements", so that the high expectations of customers, employees, and other stakeholders can be satisfied[137].
In the United States, a similar importance has been attached to the Public Benefit Corporation (PBC). The PBC is a new type of business structure deriving investment value from requiring companies to implement practices producing one or more public benefits and to operate in a responsible and sustainable manner. This for-profit corporation is slightly different from B Corp status, which is a certification from the non-profit organization B Lab that companies usually try to get to raise their

[133] Ibid.
[134] Fischer Kuh, K. Cit. pg.1594.
[135] Rimmer, M. Cit. pg.180.
Fowler, M. (2018) *Linking the Public Benefit to the Corporation: Blockchain as a Solution for Certification in an Age of Do-Good Business*, 20 Vanderbilt Journal of Entertainment and Technology Law. pp.884-885.
[136] Fowler, M. Cit. pg.884.
[137] Esty, D C. Cit.pg.190.

credibility[138]. As a matter of fact, this certification attests a company meets high standards for social and environmental performance, accountability, and transparency[139].

A Certified B Corporation is defined as "a hybrid entity […] equally focused on creating profits and addressing significant social and environmental challenges"[140].

While PBC status is a legal designation that some states recognize[141], a B Corp or Certified B Corporation is a third-party certification similar to Fair Trade or LEED[142].

Nevertheless, these designations aren't mutually exclusive and both PBC and B Corp aim at "us[ing] the power of business for the higher purpose of solving society's most challenging problems"[143].

As demonstrated, consumers attribute great importance to sustainability, so much so that "an entire sustainability market" was able to emerge even during a period of economic decline[144].

2011 for instance, saw an increase in the "construction of eco-friendly single-family homes", making up for 17 percent of "the overall American residential construction market"[145].

In the same period, "fair trade products" were gaining in popularity too, even if it was known that this label would automatically raise those products' price[146].

Since the demand for sustainably and responsibly sourced products and for shares in companies that engage in responsible practices keeps on growing, it is increasingly important for business to be able to verify that their practices are as responsible as they claim[147].

1.4.1 "Greenwashing" or "fairwashing"- when organizations exploit Voluntary Standards using labels certifying their fake adherence to environmental standards

Despite what it has been affirmed so far, the existence of multiple voluntary standards can sometimes lead to fraud and unfair misrepresentation. Indeed, organizations may try to make

[138] buildd. *PBC Company - Definition of Public Benefit Corporation & Compare PBC vs B Corp vs Nonprofits* https://buildd.co/funding/public-benefit-corporation [15/07/2022]

[139] Whittaker, M. (2022) *Public Benefit Corporation vs. B Corp: What's the Difference?* https://money.usnews.com/investing/articles/public-benefit-corporation-vs-b-corp-whats-the-difference [16/07/2022]

[140] buildd. Cit.

[141] Whittaker, M. Cit.

[142] LEED certification is the most widely used and recognized green building rating system around the world. (https://www.rts.com/resources/guides/what-is-leed-certification/)

[143] Fowler, M. Cit. pg.890.

[144] Fowler, M. Cit. pg.887.

[145] Ibid.

[146] Ibid.

[147] Fowler, M. Cit. pg.890.

themselves appear more sustainable and ethical than they actually are, using misleading advertising and labels. This practice is known as "greenwashing" or "fairwashing"[148].

The 'clean diesel' scandal is an example of greenwashing involving Volkswagen cars' production[149]. In the United States, since 2009, Volkswagen had been selling "clean diesel" vehicles which were supposed to "offer great mileage and low pollution"[150]. However, vehicles were fitted with software letting cars' pollution controls work only when being tested for emissions. At any other time, the vehicles could "freely spew hazardous, smog-forming compounds"[151].

Company executives were arrested on conspiracy charges[152] for having cheated state emissions tests and the Environmental Protection Agency announced the Clean Air Act had been violated, ordering Volkswagen to fix the affected vehicles and to pay fines as high as $18 billion[153].

Nevertheless, most greenwashing is not so evident and can be acknowledged from "subtle distinctions between marketing messages and the realities of a product"[154].

Different definitions of this phenomenon exist, but one the most outstanding derives from Jacob Vos' perspective[155]. Vos identified three types of greenwashing, three strategies to bowdlerize a corporation's acts in the face of the media, namely confusion, fronting and posturing[156].

Confusion's meaning is more similar to the concept of greenwashing that has already been outlined, since it occurs "when a firm selectively uses information to promote its green credentials that may not provide the full picture of a problem at hand"[157]. Fronting occurs when a company seeks an authoritative representation of its environmental credibility through experts' confirmation, whereas posturing consists in trying to bring internal and external stakeholders around to the ethical purpose of the firm[158].

Considering that these concepts apply both to products and to firms, suggesting they are respectively more eco-friendly than they are, or they undertake more environmental responsible choices than they really do, it is clear that greenwashing can occur both at a product and firm level.

---

[148] Fowler, M. Cit. pg.894.
[149] Fowler, M. Cit. pg.884.
[150] Plumer, B. (2015). *Volkswagen's appalling clean diesel scandal, explained* https://www.vox.com/2015/9/21/9365667/volkswagen-clean-diesel-recall-passenger-cars [16/07/2022]
[151] Ibid.
[152] Fowler, M. Cit. pg.895.
[153] Plumer, B. Cit.
[154] Fowler, M. Cit. pg.895.
[155] Vos J (2009). Actions speak louder than words: greenwashing in corporate America. Notre Dame JL Ethics Pub Policy. pg.679.
[156] Ibid.
[157]Rimmer, M. Cit.pg.309.
[158] Ibid.

The Federal Trade Commission (FTC) in the United States is responsible for strengthening consumer protection, preventing fraud and "sanctioning deceptive advertising"[159]. Several 'Green Guides' have been created, and the most recent version date back to 2012. These guidelines are not "statutory law", but they explain how companies should "address environmental messaging" in order not to convey deceptive messages[160].

The four main principles at the basis of the Green Guides are the following:

1. Any qualifications or disclosures should be sufficiently clear, prominent, and understandable to prevent deception
2. Environmental claims should clearly indicate to what they refer
3. Environmental claims should not be presented in a manner to overstate their environmental attribute or benefit expressly or by implication
4. Comparative statements should be presented in a manner that makes the basis for the comparison sufficiently clear to avoid consumer deception[161].

In the 2012 update, it was explicitly stated that unqualified general claims could no longer exist, and clear qualifications indicating a specific benefit need to be attached to general benefit claims.

In conclusion, voluntary standards systems play an important economic role, but they need to be supported by reliable and universally recognized certification[162].

1.4.2 A need for homogenization of Standard and Certification Systems

The strength of voluntary standard, certifications, and labelling systems decreases considerably when a multitude of such standards is available, preventing consumers from telling them apart and meaningfully evaluating them[163].

Early in the Chapter, it has been described how private-sector organizations (both for-profit and nonprofit), can try to hold producers accountable for the environmental and social impacts of their production practices and supply chains[164]. However, besides these entities, governmental organizations, and organizations that are somewhere in between the private and public sector, can take part in this scenario too. For instance, using *GoodGuide* online platform or app, consumers can have instant access to safe, healthy, and green products[165]. Even though the information consumers

[159] Rimmer, M. Cit. pg.310.
[160] Ibid.
[161] Rimmer, M. Cit. pg.310.
[162] Fowler, M. Cit. pg.896.
[163] Fowler, M. Cit. pg.901.
[164] Fowler, M. Cit. pg.902.
[165] Crunchbase. GoodGuide: https://www.crunchbase.com/organization/goodguide [01/08/2022]

can deal with are all credible and supported by experts' confirmation, problems arise from "information asymmetry and the difficulty of tracking a product's origins"[166].

GoodGuide's data system flaws are due to the lack of a single credible source from which data can be retrieved. Indeed, those data are caught from "over 1,000 different sources, including scientific institutions, governmental agencies, commercial data aggregators […]", and they may even not be available if companies decide not to enable critical information disclosure[167].

This is an example of some of the issues arising from data systems that do not rely on uniform standards and certifications.

The diffusion of the 'fair-trade' label is a proof of how voluntary standards can create a "market for resource protection"[168].

Nevertheless, even in this case, several fair-trade labels with confusingly similar names exist.

Another problem arises from the fact that traditional corporations can obtain both the B Corp certification and the PBCs status. The famous retailer of outdoor clothing Patagonia, for instance, is both a PBC and a B Lab-certified B Corp, whereas other major corporations do not appear in Fair Trade USA's list of certified entities, even if they comply with Fair Trade USA's requirements[169].

As a consequence, it is even more difficult for consumers to get to know the "true nature of these companies" and understand the difference between a company "that has met the corporate social responsibility requirements for each of the various fair-trade certifications" or a company that received a PBC status or B Corp certification[170].

The presence of all these market actors is misleading and could also be deceptive for consumers[171].

The PBC context may stir up uncertainty, raising the question of whether the corporation's practices are really trying to create the greater social conscientiousness they claim.

If they really aim at reaching PBC's goal of advancing a "public benefit", a more uniform certification system may need to take the place of the ones that are currently in force "both for PBCs and for the broader corporate environment"[172].

In the European context, it is worthy to cite the *Green Paper* on Corporate Social Responsibility (CSR) presented by the European Commission in July 2001[173]. Corporate social responsibility is "a concept whereby companies integrate social and environmental concerns in their business operations

[166] Fowler, M. Cit. pg.902.
[167] Ibid.
[168] Fowler, M. Cit. pg.903.
[169] Fowler, M. Cit. pg.906.
[170] Fowler, M. Cit. pg.905.
[171] Fowler, M. Cit. pg.906.
[172] Fowler, M. Cit. pg.906.
[173] Brutti, N. (2005). pp. 203-204.

and in their interaction with their stakeholders on a voluntary basis"[174]. The *Green Paper* seeks to create a framework of responsibility and competitiveness, in which the most prominent companies and multinational corporations should adopt some codes of conduct to their production practices, covering working conditions, human rights and environmental aspects[175].

As stated in the *Green Paper on Social Responsibility*, authorities and public initiatives are increasingly encouraging companies to submit reports about their social and environmental performance. An example is the European Commission's Recommendation of 30 May 2001 "on the recognition, measurement and disclosure of environmental issues in the annual accounts and annual reports of companies", which deals with the development of relevant and comparable information concerning environmental issues in the European Union[176].

In this part it has been demonstrated that today the wide variety of ways to certify corporate social responsibility, not only involves many entities and therefore, different levels of accountability, but also entails several problems[177].

Although the need for homogenization of standard certification systems has already been internationally recognized, and efforts have been made "to consolidate the public, private, and hybrid standards requirements into a "common language"[178], the unambiguousness and compulsoriness of standards is still a goal to be achieved[179].

1.5 Blockchain- a possible tool for countering information asymmetry and guarantee corporate social and environmental responsibility?

It has been stated so far that as the market value of responsible production grows, it becomes increasingly more necessary to bear out hypothetical socially and environmentally responsible practices[180]. In this context, blockchain could offer a potential solution to guarantee "such accountability in enforcing standards for certification and labelling systems". [181]

---

[174] Commission of the European Communities. 2001b. pg.6. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52006DC0136:EN:HTML [06/08/2022]

[175] Commission of the European Communities. (2001). *Final Green Paper Promoting a European framework for Corporate Social Responsibility.* https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2001:0366:FIN:EN:PDF%20 [06/08/2022]

[176] Brutti, N. (2005). Cit. pg.205.

[177] Fowler, M. Cit. pg.905.

[178] Fowler, M. Cit. pg. 902.

[179] Brutti, N. (2022). Cit. pg.21.

[180]Fowler, M. Cit. pg.886.

[181] Ibid.

Based on a digitally distributed, decentralized, public ledger, blockchain technology is independently verifiable, and this allows to improve certification systems' transparency[182].

For this reason, innovators believe this technology is suitable for a new use, which is different from the one it was conceived for, proposing the Bitcoin cryptocurrency as a tool to "track production along corporate supply chains"[183]. It would thereby be possible to verify whether companies truly implement the environmentally responsible practices they report and advertise.

Businesses like GoodGuide, as described above, have already considered the idea of using blockchain technology to track products along their supply chain for the sake of data availability and reliability issues. Provenance, a software for sustainability communications, utilizes blockchain to track "any type of product, throughout every part of its lifecycle"[184], thus enhancing reliability in reviewing products[185]. This company enables brands to communicate their social and environmental impact with shoppers, so that they can do a good deed buying a "responsible" product, and reward those environmentally friendly brands, making a positive impact on people and the planet[186].

Other fintech start-ups, large companies like Unilever and Sainsbury's, and global banks like Barclays and BNP Paribas are cooperating as well to "test whether blockchain technology can help unlock financial incentives that improve transparency and sustainability in supply chains"[187].

There are many factors supporting the positive and procompetitive effects that inserting blockchain technology in the certification process could entail[188].

First, blockchain could cover all information needed; it could provide low-cost and flexible adjustments to standards[189] and it could mitigate the costs associated with adjusting methods of measuring compliance to changing production standards.

Furthermore, it could keep track of "the entire lifespan of a product as it moves through a supply chain" and it would thereby be at the foundation of measuring adherence to "standards with which the producer may wish or be obliged to comply"[190].

Nevertheless, some obstacles still subsist concerning the role blockchain could play in changing corporate environment.

---

[182] Ibid.
[183] Ibid.
[184] Fowler, M. Cit. pg.916.
[185] Fowler, M. Cit. pg.914.
[186] Crunchbase. *Provenance* : https://www.crunchbase.com/organization/provenance [04/06/2022]
[187] Fowler, M. Cit. pg.915.
[188] Fowler, M. Cit. pg.913.
[189] Ibid.
[190] Ibid.

Among the most discouraging factors one can cite politics, regulatory approval, or the efforts that are still to be made on "custom software design and front and back-end programming to link up the new blockchain ledgers to current business networks"[191].

Although those challenges seem to impede progress, blockchain technology is still likely to yield good results in future certification systems and could also be particularly important in the PBC context. As previously affirmed, according to PBC corporate doctrine it is not necessary to have a third-party check whether a company is opting for socially and environmentally responsible practices, even if in theory their ultimate aim should be the pursuit of public benefit[192].

Therefore, it will become fundamental for PBCs to demonstrate that "they meet baseline standards for social responsibility" and they are able to provide the purported public benefit[193].

The blockchain technology could also prevent PBCs' from imposing their own sustainability standards, a risky practice that could entail even greater anticompetitive consequences than for traditional corporations[194].

The extensive implementation of blockchain technology would lead to the creation of more transparent and reliable certification systems, which would be able to mitigate the market failures of our "modern, high-transaction-cost business environment"[195].

Hence, it is important that lawyers, businesspeople, and regulators start to address the still existing obstacles to blockchain-based certification systems[196].

[191] Fowler, M. Cit. pg.916.
[192] Ibid.
[193] Ibid.
[194] Ibid
[195] Fowler, M. Cit. pg.917.
[196] Fowler, M. Cit. pg.916.

Chapter 2

Smart Grids

As seen in the previous Chapter, fostering technological innovations to counter climate change is one of the greatest challenges facing the world today.[197] In this Chapter, we will both focus on smart grids, describing how they can reduce carbon emissions and improve energy efficiency; we will outline several concrete examples as well.

2.1 A way to enable environmentally sensitive electricity distribution and consumption practices

Even though we can boast of many promising strategies helping the cause of climate change, it is common knowledge that the focus should be on accessing energy more efficiently and in smaller quantities[198].

Nowadays, new technologies are primarily designed to save energy[199]. The deployment of smart grids in high energy consuming areas like Europe and North America, is an example of such new technology, and it represents a turning point in this context[200].

A smart grid is a "two-way flow" electricity network that can "integrate the actions of all users connected to it- generators or consumers —in order to efficiently deliver sustainable, economic and secure electricity suppliers"[201].

In other words, once sensors and transmitters are introduced into the grid, they can communicate to create "near real-time energy usage data and allow for remote operation of grid components"[202].

[197] Rubin, E S. (2010) *Innovation and Climate Change.* Source: NRC. Carnegie Mellon University.pg.333.
[198] Kalkbrenner, A. (2018) Climate Change, Big Data Revolution and Data Privacy Rights. 32 J Envtl L & Pract 1 at 6 (WL).pg.4.
[199] Kalkbrenner, A. Cit. pg.9.
[200] Kalkbrenner, A. Cit. pg.4.
[201] Kalkbrenner, A. Cit. pg.5.
[202] Ibid.

Advanced metering infrastructure (AMI), a wireless network architecture, is essential to the smart grid[203]. It is thanks to AMI technologies that electricity service providers can track consumer energy usage in near real-time[204].

The United States. Department of Energy stated that:

> A truly smart grid should achieve environmental goals at lower cost than the traditional grid, be able to respond more quickly to natural or man-made outages and, overall, operate the electrical system more efficiently without reducing system cyber security or reliability[205].

The difference between a traditional electricity meter and a smart meter lies on the fact that the first one measures total electricity usage whereas the second measures a home's energy usage in near real-time, during a 15-minute interval for instance[206]. Near real-time energy consumption allows consumers to better determine their own consumption's rate, thus encouraging behavioural changes[207]. Indeed, when consumers are fully conscious of their energy usage, they may be more inclined to change their behaviour, limiting their energy consumption during expensive peak hours or making upgrades to inefficient home appliances[208].

For example, users will have the chance to turn appliances on and off remotely if the power consumption of their homes is connected to the Internet. In doing so, they could "switch off forgotten and unneeded appliances while outside the home", thus reducing both energy waste and their electric bills[209].

Moreover, these devices "will be able to monitor the health of the grid proactively", making it possible to repair pending faults and avoid service interruptions.[210]

The smart grid also allows governments, regulators, and cities to keep track of their greenhouse gas emissions, elaborate specific policies and check their compliance with all kinds of energy efficiency targets[211].

Another positive effect is related to transport grids, namely devices that detect road traffic flows and according to that data, they signal possible traffic jams or accidents, suggesting drivers they should

[203] J Harvey, S. (2014). Smart Meters, Smarter Regulation: Balancing Privacy and Innovation in the Electric Grid. 61 UCLA L Rev 2068 at 2070. pg.2072.
[204] Ibid.
[205] Ibid.
[206] Ibid.
[207] Kalkbrenner, A. Cit. pg.5.
[208] Ibid.
[209] J Harvey, S. Cit. pg.2073.
[210] Ibid.
[211] Kalkbrenner, A. Cit.pg.6.

avoid specific routes for instance[212]. In this way, the idling of vehicles and heavy trucks are reduced, with a consequent decrease of both noise and air pollution levels[213].

Economy will profit from smart grids as well. As a matter of fact, more effective grid operation will guarantee "fewer and shorter outages" and consumer behavioural changes will result in "lower energy costs and more efficient and accurate pricing"[214]. In a nutshell, smart grids' implementation will benefit society as a whole[215].

Nevertheless, since smart data offer "a very detailed picture of an individual's life and behaviour", access to personal energy consumption data is sometimes considered as an inappropriate intrusion into privacy[216].

According to the Paris Agreement, data collected by environmental smart grids are "potentially disseminated to institutional, community and other databases" and need to be integrated with data from other users and official sources[217]. This aggregation turns data into accessible information that can be "networked to distribute environmental data on an ongoing automated basis or on demand"[218]. This process of data collection, integration and dissemination represents a "bottom-up mechanism for climate justice" since it makes ordinary people more aware of environmental issues and eventually pushes them to show commitment to environmental sustainability[219].

However, active involvement of third parties focusing on energy efficiency is needed to reach all those benefits described above. Therefore, new policies facilitating research institutions and private companies' access to AMI data should be adopted [220].

In conclusion, thanks to smart grids, energy consumers can be more informed about their consumption and thus change their behaviour for the better.

Nevertheless, a widespread use of smart grids creates a potential conflict between the use of Big Data and data privacy over the use and privacy of energy consumption data[221]. Chapter 3 will be dedicated to this phenomenon.

[212] Rimmer, M. Cit. pg.380.
[213] Ibid.
[214] J Harvey, S. Cit. pg.2074.
[215] J Harvey, S. Cit. pg.2073.
[216] Rimmer, M. Cit. pg.380.
[217] Rimmer, M. Cit. pg.385.
[218] Ibid.
[219] Ibid.
[220] J Harvey, S. Cit. pg. 2076.
[221] Kalkbrenner, A. Cit. pg.4.

2.2 The role of the Internet of Things in the smart grid evolution

The Internet of Things (IoT) is a "system of interrelated computing devices, mechanical and digital machines, objects, animals or people" supplied with unique identifiers (UIDs)[222].

The interconnection of these devices allows the transfer of data over a network without the need of human-to-human or human-to-computer interaction[223].

A 'thing' in this context can even be a person with an implanted loop recorder, a farm animal with a biochip transponder, a car equipped with sensors to alert the driver when tire pressure is low; in sum, any object that was assigned an Internet Protocol (IP) address and that can, therefore, transfer data over a network[224].

As mentioned above, nowadays smart homes are equipped with appliances or some form of renewable energy resources which can be considered IoT technologies, since they allow users to upload and download data and commands[225].

This system has recently proved to be an "enabling technology for the smart grid, smart health, smart transportation, and smart environment as well as for smart cities"[226].

Since the seven already existing domains for smart grid's conceptual model do not include the IoT, many attempts have recently been made to introduce the IoT as enabling technology to the grid[227].

2.3 Some examples of inherent initiatives

2.3.1 Radio frequency identification (RFID) technology

This subparagraph will delve into Radio frequency identification devices (RFID), a pioneering invention concerning the Internet of Things.

The term *Internet of Things* itself was coined by Kevin Ashton in 1998, during his presentation at Procter&Gamble[228], an American consumer goods corporation specializing in a wide range of

[222] TechTarget Network (2022). *What is the internet of things (IoT)?* https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT [20/08/2022].
[223] Ibid.
[224] Ibid.
[225] Al-Ali, A. and Aburukba, R. (2015). *Role of Internet of Things in the Smart Grid Technology*. Journal of Computer and Communications, 3. pg.230.
[226] Al-Ali, A. and Aburukba, R. Cit. pg.229.
[227] Ibid.
[228] Ferguson, A. G. (2016). *The Internet of Things and the Fourth Amendment of Effects*. California Law Review, 104(4). pg.813.

personal care and hygiene products[229]. Ashton, an innovator and consumer sensor expert, was working on supply chain optimization and wanted to draw attention to this new technology called RFID.

RFID chips were a revolutionary innovation since they began to provide objects with unique identifiers and started therefore being used to track and monitor manufacturing processes[230].

Manufacturing parts could be tracked along the production line, speeding regulating inventory, managing real-time precision, and target retail sales at micro level, thus improving outputs[231]. Engineers also developed wireless sensor networks to monitor products, which gave impetus to factory automation process. The public sector began to adopt this technology too, with governments monitoring users of public services[232]. Nowadays, smart electricity grids supervise geographic areas and keep track of human activities, "revealing numerous personal details otherwise not observable to the public"[233].

Furthermore, since companies discovered they could get valuable information about consumer habits and preferences from these ordinary items, they decided to adapt "these industrial and governmental innovations to the consumer space" and started to take advantage of their chance to map consumers' interests[234].

RFID technology has also been fundamental to solve practical application problems, such as "assets management, working environment control, and vehicle networking"[235]. As RFID and location-based services technology are increasingly developing, RFID needs to meet other "sensing, communication, and information technologies". Indeed, according to researchers, if combined with other technologies and concepts of innovative design, RFID technology could meet many other application requirements and cover even more aspects of management and production processes[236].

It is also worthy to better explain how RFID technology can be applied to the smart grid.

One of the fields of application we will discuss is the "Power asset management".

---

[229] Fortune. *Procter & Gamble.* https://fortune.com/company/procter-gamble/#:~:text=Procter%20%26%20Gamble%20is%20an%20American,and%20James%20Gamble%2C%20a%20soapmaker**.**
[01/11/2022]

[230] Ferguson, A. G. Cit. pg.814.

[231] Ibid.

[232] Ferguson, A. G. Cit. pg.815.

[233] Ferguson, A. G. Cit. pg.816.

[234] Ibid.

[235] Wang, X., Dang, Q., Guo, J. and Ge, H. (2013). *RFID Application of Smart Grid for Asset Management.* International Journal of Antennas and Propagation. Vol. 2013, no. 2013. pg.1.

[236] Ibid.

The traditional management of electricity meters generally relies on the barcode method[237]. However, this method turned out to be inefficient and misleading at times. As a matter of fact, the barcode label could easily fall and damage- inhibiting sometimes its normal reading- and without giving the possibility to change information[238].

For these reasons, electric power companies use RFID to realize the effective management of electricity meters. After having been pasted on the meter, RFID tag allows to collect all the data of the meter[239]. Tools with RFID tags are put into a "special customized intelligent tool cabinet with RFID reader", thus, all kind of operation- e.g., when tools are taken out of the cabinet- can be recorded in real time[240]. The system can also notify whether a tool is not returned within a certain deadline through the operation authority.

RFID technology is also employed for electric power archives management, and it is composed of system and terminal management equipment. The terminal management includes RFID electronic tag, and other links that cooperate to enable "the information management in the process of file management"[241].

Another process in which RFID technology plays an important role is the power equipment inspection. Through this inspection power equipment's safety and reliability are guaranteed. At the same time, the power equipment management department works to effectively supervise inspection the personnel carry out and examine information to maximize work efficiency and precision of power equipment[242].

Briefly, "smart grid realizes the management of the whole life cycle of equipment, reduces the workload of equipment warehousing and inspection, and improves the automation level of equipment management"[243].

One can really affirm that nowadays smart grids can 'achieve intelligence', with RFID reading and writing equipment to collect data and making sure these data are truthful, stable, and reliable during the process of data transmission and conversion.

---

[237] Electronic Paper (2020). *Application and importance of RFID technology in Smart Grid* https://ee-paper.com/application-and-importance-of-rfid-technology-in-smart-grid/ [23/08/2022]
[238] Ibid.
[239] Ibid.
[240] Ibid.
[241] Ibid.
[242] Ibid.
[243] Ibid.

Furthermore, compared to the past, RFID technology can be extended to many more environments, including harsh ones, even characterized by extreme temperatures or chemical contaminants[244]. Anyway, RFID's flexible applications, increased efficiencies, and cost-effectiveness have made it popular in a variety of industries and proved the efficiency of a technology that paved the way to the IoT diffusion[245].

2.3.2 Ambient Orb - a technology to aid energy conservation

As explained in the previous paragraphs, individuals can rely on smart meters and smart appliances to get to know "detailed information about their energy use in readily understandable formats, track the energy use of particular appliances, and pre-program appliances to run (or not run)" according to electricity prices[246]. "Ambient Orb" is an example of such technology created to aid energy conversation. This device is a "frosted-glass ball that illuminates a varying degree of colours to represent critical peak demand conditions on the smart grid"[247]. In particular, it glows red when a customer is using lots of energy and prices are more expensive, whereas it turns green when energy use is low[248]. Ambient Orb's imbedded intelligence and network connection allow to produce real-time feedback from the energy grid[249], providing users with detailed information about their environmentally significant behaviour, thus encouraging them to make smarter energy consumption choices[250].

These devices have been the backbone of "residential and commercial demand response projects worldwide to show the load on the grid, manage demand and avoid brownouts"[251].

In 2008, Baltimore Gas & Electric Company (BG&E) begun an experiment called the Smart Energy Pricing (SEP). SEP was designed to study how users would "respond to a variety of smart grid stimuli" and took place from the beginning of June until the end of September[252]. Two types of

[244]Lowtry Solutions. *What is the Future of RFID Technology?* https://lowrysolutions.com/blog/what-is-the-future-of-rfid-technology/
[23/08/2022]
[245] Ibid.
[246] Fischer Kuh, K. Cit. pg.1588.
[247] Irizar-Arrieta A., Diego Casado-Mansilla D., Garaizarb P., López-de-Ipiñaa D., Retegib A. (2020). *User perspectives in the design of interactive everyday objects for sustainable behaviour*. International Journal of Human-Computer Studies. Volume 137. pg.3.
[248] Ibid.
[249] Electric Energy Online. Green Ovations: Innovations in Green Technologies. *More Power, Less Energy: Power to the People*
https://electricenergyonline.com/energy/magazine/618/article/Green-Ovations-Innovations-in-Green-Technologies.htm
[30/08/2022]
[250] Fischer Kuh, K. Cit. pg.1588.
[251] Electric Energy Online. Cit.
[252] Ibid.

dynamic pricing rate- critical-peak pricing and peak-time rebates- were controlled and two types of enabling technologies namely the Energy Orb and switches for cycling central air-conditioners were used [253].

Matching treatment and control groups were randomly selected, and load profiles were monitored and measured before and after smart grid treatments' deployment. The total number of costumers participating in the pilot was 1,375. In particular, "354 [were] in a control group, 401 on dynamic pricing rates without enabling technologies and 278 on the Energy Orb in conjunction with dynamic pricing and the remainder on the Energy Orb and cycling switches for central air conditioners"[254].

Customers in the control group remained on standard rate, with a charge of 15 cents per kWh around the clock. On the other hand, the price people on the critical-peak pricing rate had to deal with was nine times higher on the peak period on a dozen days; this was especially decided to imitate high price conditions in the PJM[255] wholesale market[256]. Lastly, "prices during off-peak hours were about six cents per kWh lower than the standard rate"[257].

Two types of peak-time rebates were tested, featuring levels that were nine times higher and twelve and a half times higher than the standard rate.

Econometric analysis of the experimental data demonstrated that for customers on dynamic pricing without enabling technology the price responsiveness stayed the same, whether they were dealing with critical-peak pricing or peak- time rebates[258]. However, users reduced their consumption during critical-peak periods by 19.6 percent on average, while the group provided with Energy Orb conveying actionable information displayed an increase of 24.9 percent of price responsiveness.

In conclusion, the SEP pilot proved how powerful dynamic pricing is, especially when attached to information-conveying technologies such as the Energy Orb[259].

2.3.3 PlanetWatch

Air emissions are tracked with a degree of precision that was inconceivable a few years ago. Nowadays regulators can plot the drift of air pollutants accurately thanks to the Gaussian plume

[253] Ibid.
[254] Electric Energy Online. Cit.
[255] PJM is a regional transmission organization (RTO) that coordinates the movement of wholesale electricity in all or parts of 13 states (Delaware, Illinois, Indiana, Kentucky, Maryland, Michigan, New Jersey, North Carolina, Ohio, Pennsylvania, Tennessee, Virginia, West Virginia) and the District of Columbia- https://www.pjm.com/
[256] Electric Energy Online. Cit.
[257] Ibid.
[258] Ibid.
[259] Ibid.

analysis[260]. Moreover, advances in meteorological modelling have further enabled the discovery of "sources and 'receptors' of air pollution"[261].

Thanks to this progress in measuring and monitoring, it will be increasingly easier to map emissions sources, and the comprehension of exposure pathways and impacts will be enhanced as well[262].

This process is fundamental since awareness of what is happening to our environment should thrust legislators to tailor policy responses to critical circumstances[263]. In other words, the improvement of our "capacity to fill information gaps in problem identification, causal specification [and] impact evaluation" should lead to the adoption of policies aiming at reducing air pollution, lowering the burden of disease attributable to it, as well as contributing to the near- and long-term mitigation of climate change[264].

Technological innovation can play a leading role in addressing societal problems such as air pollution. Industries innovations are mainly the result of consumers' desire, but it is not the case for "most environmental technologies whose function is to reduce or eliminate a pollutant discharge to the environment"[265]. For instance, most people would not pay an extra $1,000 to install air pollution emission controls on their cars unless every driver was required to do so, since, as already explained, they would think their action alone would do little both to avoid and worsen air pollution[266].

However, some companies have engaged in the fight of air pollution and have tried to implement new technologies to espouse the cause.

PlanetWatch's effort is particularly suitable to this context. As a matter of fact, PlanetWatch is a blockchain company which has developed a global network of low-cost air quality sensors to improve air quality monitoring and thus contribute to solving the public health challenge of air pollution[267]. In 2020, this company joined the French Business Incubation Centre of CERN Technologies, namely the largest fundamental physics laboratory in the world and raised 1.2 million euros in funding[268].

PlanetWatch encourages citizens to install air quality sensors and offers smart city solutions too, partnering with local government and community leaders to raise awareness on air quality issues and

---

[260] Esty, D C. Cit. pg.157.
[261] Ibid.
[262] Esty, D C. Cit. pg.157.
[263] Esty, D C. Cit. pg.160.
[264] World Health Organization. *Air pollution*. https://www.who.int/health-topics/air-pollution#tab=tab_1 [15/08/2022].
[265] Rubin, E S. Cit. pg.333.
[266] Ibid.
[267] Algorand. *PlanetWatch Environmental***.** https://www.algorand.com/ecosystem/use-cases/planetwatch [31/08/2022].
[268] Cern Accelerating science. *CERN air-quality data analysis spin-off raises 1.2 million euros in funding* https://kt.cern/content/cern-air-quality-data-analysis-spin-raises-12-million-euros-funding [31/08/2022]

to identify some sort of ambassadors who have the task of recruiting other people to support their effort[269].

Sensors are connected to PlanetWatch network and data are used in the form of aggregated, fully anonymized datasets subject to the approval of the sensor's owner and shared in accordance with privacy laws such as the European GDPR legislation[270]. Sensor owners receive an Algorand Standard Asset (ASA) called "Planet", a token reward in return for the data they gather. Algorand is a blockchain platform and cryptocurrency designed to function like a major payments processor onto which all data collected are transcribed. This "global network of nodes" is run by "universities, non-profits, research institutions, investors and cutting-edge organizations"[271]. It is thus an open-source and decentralized platform which can handle over 1000 transactions per second and finalize blocks in approximately 5 seconds.

"Every 24 hours an algorithm checks the number of data streams sent, updates the sensor score and communicates with the reward engine to send planet token rewards to sensor owner accounts[272]". Sensors' activity is evaluated every day. In particular, the sensor must deliver more than 50 percent of the expected daily data streams to earn one point. If it is not able to do so, it is not qualifying and loses one point[273].

PlanetWatch verifies whether its measurements are consistent and reliable by calibrating its data sets sensors against governmental reference stations[274]. This verification process took place in Italy, where sensors were installed both close to governmental ones, monitoring sensors' behaviour in real time conditions, and in other positions too, using different installation modes to evaluate the robustness of readings and the response of devices to specific triggers such as combustion of different fuels.

These tests proved the efficiency and solidity of their network[275].

PlanetWatch came into its home even during the recent COVID-19 pandemics. As a matter of fact, scientific research found that exposure to air pollution, and especially the risk of infection via aerosol in indoor, crowded and inadequately ventilated areas, caused an increase in COVID-19 mortality rate[276].

[269] White Paper PlanetWatch. https://www.planetwatch.io/white-paper/index-h5.html?page=1#page=64 [16/08/2022]. pp.3,11.
[270] White Paper PlanetWatch. Cit. pg.13.
[271] White Paper PlanetWatch. Cit. pg.31.
[272] White Paper PlanetWatch. Cit. pg.33.
[273] White Paper PlanetWatch. Cit. pg.51.
[274] White Paper PlanetWatch. Cit. pg.25.
[275] Ibid.
[276] White Paper PlanetWatch. Cit. pg.3.

This company filled a gap in the market by creating affordable yet advanced turnkey air purification and monitoring solutions, delivering real-time projections of infection risks via aerosol and verifying accordance with the latest air quality standards[277].

In short, by leveraging the Algorand blockchain, advanced data acquisition software developed at CERN and high-performance, yet affordable air quality sensors developed by a major research institute, PlanetWatch decentralizes, incentivizes, and gamifies air quality monitoring[278].

This company was able to find an optimal balance between data quality, network deployment time and costs[279], providing cities, industries, and citizens with accurate, timely and easy to understand information about air quality[280]. In doing so, an immutable air quality repository accessible to all participants is created[281].

To conclude, this Chapter has described the growing recognition of the importance of investing in research and development of new technologies such as smart grids- to foster or at least to monitor climate change. Technological innovation is a complex process, and its benefits are not immediately visible. Gains are often realized only with widespread adoption, which typically involves a "sequence of incremental improvements that enhance performance and reduce costs overtime"[282].

Nevertheless, in parallel with this growing interest on ways to foster such innovation, a primary concern is the potential infringement of personal data privacy that the incremental use of Big Data can entail[283].

[277] Ibid.
[278] Algorand. Cit.
[279] White Paper PlanetWatch. Cit. pg.11.
[280] Cern Accelerating science. Cit.
[281] Algorand. Cit.
[282] Rubin, E S. Cit. pp.339-340.
[283] Kalkbrenner, A. Cit. pg.6.

Chapter 3

Big Data and Privacy issues

3.1 Privacy injuries of the Information Age - Negative externalities and the *"tragedy of the commons"*

Among others, one possible definition of privacy is "the right to informational self-determination", meaning that individuals, groups, or institutions must be free to decide when, how, to what extent and for what purpose information about them is communicated to others[284]. This specific definition of privacy is related to Information Privacy, which also includes *Internet privacy*, *Financial information privacy*, *Medical privacy* and *Political privacy*.

Indeed, not only human beings but also entities such as institutions and businesses may have some information they want to disclose to the public, but also sensitive information they want to keep confidential[285].

Today, many people provide their personal data on the web or on social networks without being aware of the terms of service in force or the purposes for which those data are collected. Sometimes their consent to information sharing is simply due to their will to get rid of the temporary consent screens -cookies- that block the page they are surfing on.

In doing so they accept terms and conditions that are too vague or too technical, and what is worse is that sometimes they click on them without reading[286].

This type of information matches well with the commercial dimension. Indeed, data mining makes it possible to enhance virtual commerce, reduce errors and unnecessary costs as well as attract customers and gain their trust[287].

Analysts around the world studied several economic benefits arising from the use of data, underlying that data mining could support and benefit at least seven sectors of the world economy, such as education, transport, electricity, gas and oil, health care, consumer finance and products[288].

---

[284] Zeadally, S, Pathan, A, Alcaraz, C, and Badra, M. (2013). *Towards Privacy Protection in Smart Grid.* Article *in* Wireless Personal Communications. pg.5.
[285] Ibid.
[286] Orefice, M. Cit. pg.80.
[287] Orefice, M. Cit. pg.123.
[288] Ibid.

Ideally, people reveal their needs by expressing preferences, thus data can be used to envisage more efficient services or improve government policies for the benefit of community as a whole.

Besides implementing economic development in the public and private sector, the use of data could thereby improve everyday life in terms of quality and encourage the exercise of fundamental rights[289].

Since data are information, their knowledge is fundamental to exercise one's right to freedom of expression, and at the same time, they fuel information economy generating new knowledge and greater profits[290].

Nevertheless, Big Data cannot be simply depicted as facilitators of fundamental rights. On the contrary, they are often scenarios of their violations. Big Data can be detrimental to individuals' privacy, revealing confidential information, which as such must be protected and anonymised so that the individual to whom it refers is not identifiable.[291]

Privacy injuries, much like environmental damage, qualify as "negative externalities"[292]. Negative externalities exist "whenever someone utilizes a resource but is able to impose on others the costs of that use"[293].

Pollution is the traditional example of a negative externality. A polluter focuses his choices only on the direct cost and profit opportunity derived from production, without considering the indirect costs that are inflicted on people harmed by the pollution he or she caused[294].

To solve this problem, polluters or companies in general, should be forced to "bear or internalize the costs of the pollution" they are generating[295].

If these privacy-infringing entities continue unchecked, it is likely they will demolish the "resources on which they themselves depend", creating what is regarded as *the tragedy of the commons*[296].

The tragedy of the commons is an economics phenomenon demonstrating "how economically rational, self-interested use of a commonly owned resource can result in the destruction of that resource"[297].

This concept was first formulated from an essay by the American ecologist Garrett Hardin[298].

---

[289] Orefice, M. Cit. pg.124.
[290] Orefice, M. Cit. pg.134.
[291] Orefice, M. Cit. pg.136.
[292] Hirsch, D. (2006) *Protecting the Inner Environment: What Privacy Regulation Can Learn from Environmental Law*. Georgia Law Review, Vol. 41, No. 1, pg.10.
[293] Hirsch, D. Cit. pg.23.
[294] International Monetary Fund. *Externalities: Prices Do Not Capture All Costs.* https://www.imf.org/external/pubs/ft/fandd/basics/external.htm [16/09/2022]
[295] Hirsch, D. Cit. pg.23.
[296] Hirsch, D. Cit. pg.10.
[297] Hirsch, D. Cit. pg.24.
[298] Hirsch, D. Cit. pg.24.

Hardin described a situation in which all cattle herders allowed their flock to graze on a common field of grass. The ecologist stated that according to the point of view of each single cattle herder, it was reasonable to increasingly add animals to the cattle. In this way, the cost deriving from the using up of the grass could be split among all those shepherds having the same right to make their cattle graze in the field[299]. Nevertheless, all the grass would be eaten at the end, and all shepherds would lose access to that public resource.

In short, if everyone acts according to his or her own self-interest, this behaviour will result in a harmful and collectively ruinous over-consumption[300].

This concept is the perfect description of what takes place when a website gathers and sells personal information about one of its users, or when an Internet marketer or data miner exploit this information, they "impose a negative externality on consumers"[301].

In other words, these industries benefit from the information they gather, but they do not have to bear the costs they impose, considering that they cause individuals to lose a degree of privacy[302].

An over exploitation of personal data will thus end up causing troubles to those industries who are themselves at the bases of this exploitation[303].

According to researchers, this phenomenon is already taking place. Citing Harris survey "92 percent of consumers are 'concerned', and 67 percent are 'very concerned' about misuse of their personal data online", which means that people are somehow discouraged from relying on the Internet more than they usually do because of privacy-related fears[304].

Consequently, consumers will be increasingly prone to abandon e-commerce or other activities they were used to do online, and get back to their "real equivalents", that do not put their privacy at risk. In this way, consumer trust- that is to say, the commons on which all data driven industries depend on- will be weakened.

Nowadays, it is a common belief that the Big Data Revolution has caused damage to privacy as never before[305].

---

[299] Ibid.
[300] Hirsch, D. Cit. pg.24.
Investopedia. *Tragedy of the Commons: What It Means in Economics*
https://www.investopedia.com/terms/t/tragedy-of-the-commons.asp
[16/09/2022]
[301] Hirsch, D. Cit. pg.28.
[302] Ibid.
[303] Hirsch, D. Cit. pg.29.
[304] Litan, R. E. (2001). *Law and Policy in the Age of the Internet*. pg.1058.
Hirsch, D. Cit. pg.29.
[305] Hirsch, D. Cit. pg. 30.

This phenomenon gave birth to a debate between the "two sides of the coin", namely the need to protect privacy as a fundamental value of democratic societies, and concerns about the potential negative effects regulatory reforms could provoke on firms and businesses[306].
These are exactly the issues that environmental law and policy have been wrestling with for decades and we will analyse them in paragraph 3.4.

3.2 Some existing and proposed limits on the collection or use of personal information related to RFID technology and smart grids (privacy harms)

Though Big Data with its promising economic and social benefits has proved to be a driving force, it also triggers users' concerns about their own privacy[307].
As previously mentioned, the initial goal of collecting electricity usage information to generate an electricity profile has now become a source of behavioural, personal and lifestyle information with an immense potential[308].
Furthermore, the level of personal information- including intimate details of daily life- will dramatically increase as the grid's network will keep on growing.
Among the most serious threats for the privacy of smart grid's users we can cite: "cyber-attack and intrusion, identity theft, tracking and observing the behavioural patterns of the consumers and the appliances being used, and real time spying and surveillance"[309].
In terms of legislation, Big Data challenges the Fair Information Practices (FIPs), a founding principle of all modern privacy law[310]. FIP is "a general term for a set of standards governing the collection and use of personal data and addressing issues of privacy and accuracy"[311].
This principle is interpreted in different ways, and it takes on diverse names according to different organizations and countries. In the UK they talk about "Data Protection", the European Union refers

[306] Hirsch, D. Cit. pg. 31.
[307] Rubinstein, I. S. (2013). *Big Data: The End of Privacy or a New Beginning?* International Data Privacy Law, Volume 3, No 2. pg.74.
[308] Zeadally, S, Pathan, A, Alcaraz, C, and Badra, M. pg.8.
[309] Ibid.
[310] Rubinstein, I. S. Cit. pg.74.
[311] TechTarget. *Fair Information Practices (FIP).* https://www.techtarget.com/whatis/definition/Fair-Information-Practices-FIP#:~:text=FIP%20(Fair%20Information%20Practices)%20is,issues%20of%20privacy%20and%20accuracy. [26/09/2022]

to it as "Personal Data Privacy," whereas the OECD has drawn up “Guidelines on the Protection of Privacy and Transborder Flows of Personal Data”[312].

Nowadays, one of the most prominent privacy laws in the world is the European Union Data Protection Directive 95/46 EC (DPD), which was replaced in 2012 by a new Regulation elaborated and released by the European Commission[313].

Nevertheless, even if this Regulation was created for the purpose of trying to make up for some deficiencies of the DPD as well as solving “issues associated with targeting, profiling, and consumer mistrust”, it depends too much “on the discredited informed choice model”, thus failing to fully address the overwhelming Big Data phenomenon[314].

The main problem is that Big Data not only makes it possible to re-identify individuals to which data are referred by using non-personal data, but it also makes aggregation more “granular, more revealing, and more invasive” through relentless monitoring, and sophisticated analytic abilities[315].

In this way, re-identification worsens aggregation-associated harms by allowing data controllers to add more characteristics to an individual’s profile, connecting each person to at least “one closely guarded secret”[316]. This could be all kind of private information -e.g., concerning medical conditions, family history, or personal preferences- that if revealed, may not simply provoke a privacy breach but also a concrete harm[317]. All these companies combining their data stores will create a single, massive database that Ohm named the “database of ruin”[318].

Another concern Big Data raises, relies on the fact that decisions based on data mining, which are mostly invisible to their subjects, are increasing in precision and scope, thus fuelling the development of automated decision-making process[319]. Those decisions could concern “credit ratings, job prospects, and eligibility for insurance coverage or welfare benefits”, thus all important private-life choices which are more and more unwittingly entrusted to “automated processes based on algorithms and artificial intelligence”[320].

Data aggregation and the fact that just a few people can access Big Data through non-negotiated forms of user profiling, inevitably changes the order and balance of the digital ecosystem.

---

[312] Ibid.
[313] Rubinstein, I. S. Cit. pg.74.
[314] Rubinstein, I. S. Cit. pg.74.
[315] Rubinstein, I. S. Cit. pg.77.
[316] Ohm, P. (2012). Harvard Business Review. *Don’t Build a Database of Ruin.* https://hbr.org/2012/08/dont-build-a-database-of-ruin [27/09/2022]
[317] Ibid.
[318] Ibid.
[319] Rubinstein, I. S. Cit. pg.77.
[320] Ibid.

Indeed, today access to data is a powerful instrument as it corresponds to a form of influence: people holding aggregated data not only have the capacity to control the market but also possess knowledge and therefore money.

Moreover, the collection of new types of personal environmental information can leave room for the risk of government access to that information[321].

By citing Professor Daniel J. Solove:

> The increasing amount of personal information flowing to the government poses significant problems with far-reaching social effects. Inadequately constrained government information-gathering can lead to at least three types of harms. First, it can result in the slow creep toward a totalitarian state. Second, it can chill democratic activities and interfere with individual self-determination. Third, it can lead to the danger of harms arising in bureaucratic settings. Individuals, especially in times of crisis, are vulnerable to abuse from government misuse of personal information[322].

As we will discuss in the next paragraph, in the United States the Fourth Amendment establishes that the "government does not need a warrant to search an individual's garbage, [nor it needs] a warrant to obtain information provided by individuals to third parties".[323]

All the privacy issues cited above are further confirmed by a recent Privacy Impact Assessment (PIA) released by the Privacy Sub-Group of the Cyber Security Working Group.

A PIA is a detailed assessment that can be recommended by different authoritative sources for the purpose of determining if systems and the organizations which run them, conform with federal laws, regulations, and security policies[324].

Focusing on concerns related to consumer-to-utility information exchanges in the United States' smart grid, this survey found out that some of the most feared factors are the incomprehensive and inconsistent definitions of personally identifiable information, the lack of standards, privacy policies, or procedures by the entities involved and by States[325].

As a matter of fact, despite the 2000 resolution of the National Association of Regulatory Utility Commissioners (NARUC) stating the impelling need to adopt privacy principles, "only a few State utility level commissions actually started to assess privacy issues associated with the smart grid"[326].

---

[321] Fischer Kuh, K. Cit. pg.1600.
[322] Fischer Kuh, K. Cit. pg.1601.
[323] Fischer Kuh, K. Cit. pg.1604.
[324] Science Direct. *Privacy Impact Assessment.* https://www.sciencedirect.com/topics/computer-science/privacy-impact-assessment [28/09/2022]
[325] Zeadally, S, Pathan, A, Alcaraz, C, and Badra, M. pg.7.
[326] Zeadally, S, Pathan, A, Alcaraz, C, and Badra, M. pg.8.

California is one of those States that have set guidelines aiming at both inquiring into the way in which online entities collect and use personal information and checking whether they guarantee adequate information privacy protection.

Furthermore, this State ensures compliance with eight Fair Information Practice (FIP) principles- e.g., transparency, individual access to see and copy information stored on an individual, limited types of information that may be collected on an individual, data quality and integrity, security, accountability, and auditing etc.- as well as with the California Consumer Privacy Act (CCPA)[327].

The CCPA is a state privacy law that has been effective since January 1, 2020, granting consumers more control over the personal information that businesses collect about them[328].

This regulation will be analysed in subparagraph 4.3.2 as a good example of the implementation of the privacy "right to opt-out", namely the right not to use smart meter technology.

Indeed, for the time being, state public utility commissions are the main developers of smart meter privacy protections, adopting new privacy policies targeted at smart meter technology[329].

RFID technology is not exempt from privacy concerns either.

Even though at the federal level arguments in favour of the need for technology to develop and for industry self-regulation have prevailed, in some cases States have not hesitated to impose privacy-driven restrictions on the use of RFID technology[330].

States can restrain RFID technology's implementation by "imposing conditions on the use of RFID in driver's licenses or other state-issued identification documents, barring the required implantation of an RFID device, criminalizing the use of RFID technology to commit fraud or identity theft" or again introducing more general laws prohibiting the process RFID technology employs to obtain information[331].

Even though these state limitations do not specifically point at standing in the way of RFID technology's use, some "law restrictions are broad enough to potentially frustrate such efforts"[332].

Moreover, government or companies are not authorized to read "commercial RFID identification devices that they did not issue" apart from cases in which this is extremely necessary, such as "in the course of an act of good faith security research, experimentation, or scientific inquiry"[333].

---

[327] Ibid.

[328] State of California Department of Justice. *California Consumer Privacy Act (CCPA).* https://oag.ca.gov/privacy/ccpa [28/09/2022]

[329] Fischer Kuh, K. Cit. pg.1616.

[330] Fischer Kuh, K. Cit. pg. 1611.

[331] Ibid.

[332] Fischer Kuh, K. Cit. pp. 1611-1612.

[333] Fischer Kuh, K. Cit. pg.1612.

These types of regulations could thus interfere with the useful work of RFID technology in speed limits or anti idling laws' enforcement, or even with the use of real information concerning individual environmental behaviours to help the design of more appropriate and behavioural-related policies.

If in New Hampshire, for example, municipalities cannot develop parking permits equipped with RFID, the city of Hoboken, New Jersey, has already adopted an innovative radio frequency identification (RFID) solution to manage its on-street residential parking system[334].

As prices of parking permits started to increase in Hoboken, officers realized that illegally issued and counterfeit permits were increasing too[335]. Consequently, it was more and more difficult for officers to tell real permits apart from fake ones, as well as to distinguish residents' permits- which were entitled to extended parking privileges- from those of city visitors[336].

Thanks to the synchronization of a software called PayLock's RFID Permit Management, and Symbol RFID rugged mobile computers, Hoboken parking officers could rapidly read the parking permit information stored on the RFID tag, and instantly verify whether a permit was real or not[337].

Indeed, RFID tags contained in the parking permits were endowed with an identification number stored in a database. In this database all the necessary information concerning vehicles and the kind of permit associated to them were gathered, which made it possible to identify where a vehicle could legally park.

In this way, the efficiency and effectiveness of the city's parking enforcement officers was enhanced.

Unlike for smart meters, which have seen some of their potential environmental applications widely recognized, and privacy protections trying to preserve these applications, the potential benefits of RFID for regulating environmentally significant individual behaviours have not drawn the same interest nor they have been "widely recognized or taken into account in crafting RFID privacy measures"[338].

This due to the fact that, as we have already explained, smart meters involve programs providing individuals with "energy consumption data in an accessible, thoughtful format" that encourages conservation behaviours[339].

This element justifies the special consideration policymakers have for the benefits resulting from smart meters' deployment, in contrast to RFID technology ones.

---

[334] Government Technology. (2010). *Hoboken, N.J., Battles Parking Permit Counterfeiting With RFID System.* https://www.govtech.com/public-safety/hoboken-nj-battles-parking-permit-counterfeiting.html [29/09/2022]

[335] Government Technology. Cit.

[336] Government Technology. Cit.

[337] Ibid.

[338] Fischer Kuh, K. Cit. pg. 1613.

[339] Fischer Kuh, K. Cit. pg.1614.

Privacy protections for smart meters have acknowledged and largely preserved this favourable function, even if privacy policies nonetheless impose some constraints on the potential for smart meters to support voluntary energy conservation.

Clearly, since these policies undermine the development and use of home energy management systems, they can consequently lead to a decrease in users' number, by allowing "customer opt-out". Moreover, by shaping environmental agencies' access to smart meter data, they inevitably affect smart meter information's use to regulate environmentally significant individual behaviour[340].

3.3. The Naperville Case and its implications

Naperville is a suburban community located outside of Chicago city, in Illinois State.

In recent years, this city has witnessed an increase in smart meters' deployment.

This process was accelerated by the American Recovery and Reinvestment Act, a decision adopted in 2009 by the United States Department of Energy (DOE). Approximately $3.4 billion were allocated to the Smart Grid Investment Grant Program, which was intended to pave the way to new projects including Naperville's Smart Grid Initiative (NSGI)[341].

The NSGI modernized Naperville's electrical grid, providing customers with digital smart meters that collected energy-consumption data every 15 minutes[342].

The project also entailed a City-wide access to a customer web portal where house information from the smart meters on electricity consumption and costs was registered[343]. This constant data collection combined with "the unique energy-consumption patterns of various home appliances", made it possible to identify which and when those appliances were used[344]. Consequently, it was easy to deduce which activities were taking place inside the house, understand if residents were sleeping or eating or again conclude if they were at home or not[345].

However, the city guaranteed that all these information "would not be provided to law enforcement without a warrant"[346].

---

[340] Fischer Kuh, K. Cit. pg.1616.
[341] Naperville Smart Meter Awareness v. City of Naperville, 11 C 9299, 3 (N.D. Ill. Mar. 22, 2013)
[342] Ibid.
[343] Ibid.
[344] Ibid.
[345] Ibid.
[346] Ibid.

Customers could not opt out of the smart-meter program, but they could decide to pay a one-time fee together with a monthly one, if they wanted to deactivate the transmit functions of the meter, which also implied a manual monthly reading by a utility employee[347].

Despite this program aimed at increasing energy efficiency and reducing emissions by empowering costumers and "provid[ing] them with more tools [and] information" to manage their own electricity consumption and costs", some people expressed concerns about the privacy of their data[348].

A group representing several citizens, called Naperville Smart Meter Awareness (NSMA), sued the city in federal district court, asserting smart meters installations violated the "Fourteenth Amendment right to Due process, the Fourth Amendment's prohibition of governmental searches, and the Americans with Disabilities Act (ADA)"[349].

According to the plaintiff, the fees imposed to those willing to turn off the transmit option on the digital meters were discriminating against disabled residents "who [we]re especially threatened by health risks related to smart meters"[350].

Their claim was based on the fact that radiofrequency radiation produced by radio signals to communicate information to the utility company, could "interfere with medical devices and increase cancer risk"[351]. NSMA also argued that discrimination occurred even because some customers with medical issues were forced to pay the fees[352].

The district court's initial decision "never reached the merits of the ADA claims" which were judged as "improper pleadings". The two remaining claims were judged in the same way.

Indeed, the Due Process claim was dismissed because of the lack of identifiable "cognizable liberty or property interest[353]", whereas the district judge affirmed there was no violation of "the Fourth Amendment's prohibition against unreasonable search and seizure" as the plaintiffs could have no "reasonable expectation of privacy" concerning the data which were transmitted to the utility[354].

On review, the Seventh Circuit analysed whether smart meters' installation violated the Fourth Amendment or a similar clause in the Illinois Constitution[355].

---

[347] Vergason, D. *Preventing the impending death of privacy by the Smart Grid.* Lewis & Clark Law School. Environmental Law, 2021, Vol. 51, No. 2 (2021). pg.559.

[348] U.S. Department of Energy. Electricity Delivery and Energy Reliability. Final Submitted to NREL .(2011). City of Naperville Case Study. At the Forefront of the Smart Grid: Empowering Consumers in Naperville, Illinois. pg.2.

[349] Vergason, D. Cit. pp.559-560.

[350] Vergason, D. Cit. pg.560.

[351] Ibid.

[352] Ibid.

[353] Ibid.

[354] Ibid.

[355] Ibid.

The court did not support the federal district court's and come to the conclusion that, since smart meters interfered with "reasonable expectations of privacy", their use had to be regarded as a search subject to Fourth Amendment constraints[356].

As a matter of fact, all the collected data were kept for over three years, and since information was updated every fifteen-minutes, they could reveal a great deal of "intimate personal details"[357].

Nevertheless, even though the data collection constituted a search, "the significant government interests in the program and the diminished privacy interests at stake" made the search reasonable and thus "constitutionally permissible" [358].

Moreover, the court observed that the voluntary transfer of information to a third party was not an issue since the utility was a government's property and "information given voluntarily to a third party, such as a privately owned utility, could normally be transferred to the government without constitutional concerns or restrictions"[359].

The Supreme Court ruled that Naperville's residents had given up any expectation of privacy concerning the transfer of data gathered by smart meters from the moment they started to voluntarily share it with the utility. As a matter of fact, the entire smart meters' infrastructure was considered a "third party" for purposes of Fourth Amendment analysis.

This case demonstrates that whenever individuals decide to share information with third parties in exchange for services, be those entities communications providers or financial institutions, they turn over any reasonable expectation of privacy in the information they gave[360].

"The Naperville case is illustrative of the ongoing battle in many parts of the country over the smart grid and its implementation"[361].

Consumers' privacy concerns were not adequately considered in this judgment, and they should therefore turn to legislative measures to try to get adequate safety for their personal information[362].

---

[356] Yale journal on regulation/Bernard Bell**.** (2018). *Too Smart by Half?: Naperville Smart Meter Awareness v. City of Naperville*
https://www.yalejreg.com/nc/too-smart-by-half-naperville-smart-meter-awareness-v-city-of-naperville/
[13/09/2022]

[357] Vergason, D. Cit. pg.560.

[358] Justia US Law. *Naperville Smart Meter Awareness v. City of Naperville, No. 16-3766 (7th Cir. 2018)*
https://law.justia.com/cases/federal/appellate-courts/ca7/16-3766/16-3766-2018-08-16.html
[13/09/2022]

[359] Vergason, D. Cit. pg.561.

[360] Yale journal on regulation/Bernard Bell**.** Cit.

[361] Vergason, D. Cit. pg.562.

[362] Ibid.

Unfortunately, the failure of courts to deal with users' concerns have brought many American communities to adopt laws "banning smart meter installation outright or making their installation optional"[363].

The lack of a warrant requirement for a government search of customer's electricity data is deeply concerning, especially because if individuals fear this system and argue against it, it is likely that future technological developments related to the electrical grid benefits such as the reduction of carbon resources use, would come to a standstill[364].

3.4 Methods of protecting data and approaches to protect privacy in Smart Grids

After having described the persistent tension existing between privacy and information-based technologies, this part will outline different approaches and techniques aiming both at promoting environmental protection and safeguarding costumers' sensitive data.

It is worthy to note that two generations of environmental law can be distinguished in the United States.

The first generation of environmental law dates to the 1970s and is based on "a top-down regulatory model in which government pushed emitters to adopt specific pollution control technologies [365]".

The 1970s was a seminal decade for environmental protection where laws specifying how much pollution could be caused or which pollution-control technologies had to be used, were adopted[366]. All these laws were categorized as *command-and-control regulations.*

With the adoption of command-and-control regulation, firms are not only required to take on the social costs of pollution by installing anti-pollution equipment, but they also have to pay penalties if they do not respect pollution limits[367].

First government officials determine which industry must reduce its emissions, then regulators define the so called "reference technology", namely the top-of-the-line technology for controlling pollution in that field[368]. At this point, government officials either require all the industry's facilities to adjust

[363] Ibid.
[364] Ibid.
[365] Hirsch, D. Cit. pg.31.
[366] Khan Academy. *Command-and-control regulation.* https://www.khanacademy.org/economics-finance-domain/microeconomics/market-failure-and-the-role-of-government/environmental-regulation/a/command-and-control-regulation-cnx [22/09/2022]
[367] Ibid.
[368] Hirsch, D. Cit. pg.33.

to the reference technology or make them not to pollute more than they would have done if they had installed the reference technology[369].

Despite being easily manageable and enforceable, economists have drawn attention to at least four negative aspects related to this approach.

First, it does not encourage industries to continue to invest in protecting the environment. Indeed, once they have satisfied the command-and-control regulation's requirements, industries usually do not push themselves beyond nor are willing to enhance their modus operandi[370].

Second, command-and-control regulation requires all the concerned industries to reach the same standard, or to install the same reference technology.

In this way, industries means are not considered at all, since no distinction is made between "firms that would find it easy and inexpensive to meet the pollution standard—or to reduce pollution even further—and firms that might find it difficult and costly"[371].

Third, these regulations are drawn up by legislators and the Environmental Protection Agency, so it is inevitable that they will somehow be biased and "subject to [political] compromises"[372].

Finally, this method is not able to keep pace with industries' innovations, meaning that when a technology standard is defined and announced, changes and new innovative technologies in the industry are just around the corner.

In summary, top-down regulation proves not to be the best solution for regulating the highly dynamic and competitive digital economy.

On the contrary, experts maintain that the so called "second generation" regulations are more appropriate to this matter, as they provide strong environmental protection while being flexible and cost-effective[373].

Steering away from the single government-chosen technology standard, second generation regulations allow industries to find out and implement their own approaches aiming at reach environmental goals[374].

In doing so, facilities are not led to a standstill nor blocked at the presumed "best" technology.

[369] Hirsch, D. Cit. pg.33.
[370] Khan Academy. Cit.
[371] Ibid.
[372] Ibid.
[373] Hirsch, D. Cit. pg.32.
[374] Hirsch, D. Cit. pg.38.

On the contrary, they are encouraged to innovate and even to "identify the lowest cost reducers among them and have those entities make the majority of the reductions"[375] for the purpose of producing environmental gains.

Moreover, second generation initiatives enable companies to identify the reference technology themselves, without having to deal with delays related to government's decision-making process[376].

Experience has demonstrated that those strategies are also more politically feasible than command-and-control ones because of the "widespread industry and public sentiment against government intervention in the digital economy"[377].

It is worthy to note that another instrument may also have potential to protect informational privacy if effectively employed.

We are talking about the environmental covenant approach, which consists in government officials cooperating with the regulated industry to draft an agreement on pollution reduction[378]. Sometimes, an environmental group can be called into question, and be invited to play the role of a third-party observer which can also "go public and discredit the process if it smells a 'rat'[379]".

If we look from a business' perspective, covenants are more practical and viable, that is why industries are more inclined to hammer out a covenant than a command-and-control strategy[380].

Indeed, firms can easily and flexibly decide how to achieve their environmental objectives which are usually represented by benchmarks or performance goals, instead of detailed, technology-based requirements[381].

The Dutch were among the first to implement this method with their Energy Efficiency Benchmarking Covenant. Dating back to 1999, the Dutch government negotiated the Energy Efficiency Benchmarking Covenant with some Dutch industry associations[382].

This agreement required "member companies to systematically improve their energy efficiency rate per unit of product and to scrupulously control their energy use[383]".

---

[375] Ibid.
[376] Hirsch, D. Cit. pg.38.
[377] Hirsch, D. Cit. pg.40.
[378] Hirsch, D. Cit. pg.51.
[379] Hirsch, D. Cit. pg.52.
[380] Ibid.
[381] Ibid.
[382] Iea (2017) *Energy Efficiency Benchmarking Covenant* https://www.iea.org/policies/1605-energy-efficiency-benchmarking-covenant [24/09/2022]
[383] Ibid.

Companies deciding to take part in the covenant did not have to pay any national energy tax nor add any new efficiency or CO2 targets or ceilings[384]. In addition, they were not required to define theoretical goals, they just had to try to reach nearly the same level of their best international competitors[385].

In the United States, Pollution Release and Transfer Registers (PRTRs) constitutes another second generation environmental method which also qualifies as a useful model for privacy protection[386]. PRTRs are "publicly accessible database or inventory of chemicals or pollutants released to air, water and soil and transferred off-site for treatment" obliging industries to quantify their chemicals releases and to communicate them to governments on a regular basis[387].

By noticing the public about pollution releases, PRTRs induce these industries to pollute less[388].

Another similar American initiative is the Emergency Planning and Community Right to Know Act (EPCRA). From 1986 until now, this act asks companies to report the quantity of hazardous chemicals they have released or transferred off-site in a year[389] and gathers all this data into a publicly available database called Toxic Release Inventory (TRI). Moreover, the EPCRA publishes an annual report indicating the companies that have released the most toxic substances[390].

It has been proved that, thanks to the TRI, toxic releases were reduced[391]. Indeed, if a company appears on that list, it would not just undoubtedly be discredited but it would also lose its consumers' trust.

If we turn our attention on privacy issues, we could make a parallelism between those industries we have talked about so far and information-based businesses.

Indeed, "just as no smokestack company wants to be known as a big polluter, no information-based business will want to be known as one that has [disclose] large amounts of personal information"[392].

---

[384] W. Jeffrey Howard, Phillip Townsend Associates. *Execution Experience with the Dutch Energy Efficiency Benchmarking Covenant between the Government and the Chemical Industry*. pg.155 https://webcache.googleusercontent.com/search?q=cache:LPx2SFlFlnYJ:https://aceee.org/files/proceedings/2001/data/papers/SS01_Panel2_Paper15.pdf&cd=7&hl=it&ct=clnk&gl=it
[25/09/2022]

[385] Ibid.

[386] Hirsch, D. Cit. pg.57.

[387] OECD. *Introduction to Pollutant Release and Transfer Registers (PRTRs).* https://www.oecd.org/env/ehs/pollutant-release-transfer-register/introductionto-pollutant-release-and-transfer-registers.htm
[25/09/2022]

[388] Hirsch, D. Cit. pg.57.

[389] Ibid.

[390] Ibid.

[391] Ibid.

[392] Hirsch, D. Cit. pg.58.

This claim is supported by recent studies underlining that costumers will logically steer away from companies that are more inclined to data spills.

In this context, pollution release records could come to our aid, as their example could be applied to protecting informational privacy. It has indeed been proposed to create a Data Release Inventory (DRI), a report functioning as the TRI, requiring information-based business to report the amount of personal information they released annually[393]. This report should also indicate whether data disclosure was intentional or not- e.g., data security breaches- and should be publicly spread by government officials who, for their part, should publicize an "annual ranking of individual company performance"[394]. We believe that, as with the TRI, this initiative could further enhance the protection of personal information.

In summary, as demonstrated for pollution reduction, enhanced privacy protection will depend on the development of new technologies which will, in turn, need regulatory methods fostering innovation, not constraining it[395].

Privacy regulations especially if too strict, could impede the development of new technologies which would be essential to "give consumers greater power over their information without, at the same time, impeding the flow of information that now facilitates commerce"[396].

In recent years, researchers have been working on finding out a model for guaranteeing customers' anonymity, in order to keep private those real data that sometimes companies publish.

As one may infer, anonymization is the "process of modifying personal data in such a way that individuals cannot be re-identified and no information about them can be learned"[397].

In general, perfect anonymization is hard to reach without compromising a data set's integrity.

This scenario is further complicated by Big Data and the huge amount and variety of information they involve.

On the one hand, a "low level anonymization" such as suppressing direct identifiers through a simple de-identification, cannot guarantee non-identifiability[398]. On the other, "too strong anonymization may prevent linking data on the same individual- or on similar individuals - coming from different sources and, thus, thwart many of the potential benefits of big data"[399].

---

[393] Ibid.
[394] Hirsch, D. Cit. pg.58.
[395] Hirsch, D. Cit. pg.36.
[396] Ibid.
[397] The European Union Agency for Cybersecurity (ENISA). (2015). *Privacy by design in big data: An overview of privacy enhancing technologies in the era of big data an alytic.* PO Box 1309, 710 01 Heraklion, Greece. pg.27.
[398] Ibid.
[399] Ibid.

What is certain is that, since anonymization strategies change original data to avoid personal information's spilling, a tension between utility and privacy inevitably emerges[400].

Thus, to deal with this tension, two methods- the "utility-first approach" and the "privacy-first approach" come into play. These two anonymization strategies try to take on the new challenge of safeguarding costumers' privacy and guaranteeing, at the same time, the minimum loss of accuracy.

Most data releasers today- e.g., national statistical offices- usually employ the so called "utility-first approach", since delivering useful data is their "raison d'être"[401].

This approach is an anonymization method which uses a heuristic parameter choice and is run on the microdata set[402].

Disclosure risk is then measured through an empirical estimation of the risk of re-identification, namely verifying if the record linkage between the original and the anonymized data sets is possible[403]. If the resulting risk is considered too high, the anonymization method needs to be "re-run[ed] with more privacy-stringent parameters and probably with more utility sacrifice"[404].

On the contrary, the privacy-first approach is "enforced with a parameter that guarantees an upper bound on the re-identification disclosure risk and perhaps also on the attribute disclosure risk"[405].

A model-specific anonymization method with parameters taken from the model's ones are used to achieve this enforcement[406].

Privacy-first anonymization models that have been developed and implemented are for example the "ε-differential" privacy model and the "*k*-anonymity" model and its extensions, which we will describe below[407].

Replacing the first and last names of the individuals that constitute a dataset with bogus names is not sufficient to completely mask them. As a matter of fact, even though all explicit identifiers, such as name, address and telephone number are cancelled, the remaining data can sometimes still be used to "re-identify individuals by linking or matching the data to other data or by looking at unique characteristics found in the released data"[408].

---

[400] ENISA. Cit. pg.28.
[401] ENISA. Cit. pg.29.
[402] Ibid.
[403] ENISA. Cit. pg.29.
[404] Ibid.
[405] Ibid.
[406] Ibid.
[407] Ibid.
[408] Sweeney, L. (2002). *k-Anonymity: A model for protecting privacy*. International Journal on Uncertainty, Fuzziness and Knowledge-Based Systems. pg.2.

To explain how the *k*-anonymity model works, it is useful to look at the chart below, and to focus our attention on the gender and race descriptors. These labels are referred to as "quasi-identifiers" in our context [409].

	Race	Birth	Gender	ZIP	Problem
t1	Black	1965	m	0214*	short breath
t2	Black	1965	m	0214*	chest pain
t3	Black	1965	f	0213*	hypertension
t4	Black	1965	f	0213*	hypertension
t5	Black	1964	f	0213*	obesity
t6	Black	1964	f	0213*	chest pain
t7	White	1964	m	0213*	chest pain
t8	White	1964	m	0213*	obesity
t9	White	1964	m	0213*	short breath
t10	White	1967	m	0213*	chest pain
t11	White	1967	m	0213*	chest pain

Figure 2 Example of *k*-anonymity, where *k*=2 and QI={*Race*, *Birth*, *Gender*, *ZIP*}

Source: Sweeney, L. Cit. pg.9.

"Quasi-identifiers are attributes in the original data set that [if combined] can be linked with external information to re-identify the subjects to whom the records in the original data set refer [410]".

The main difference between identifiers and quasi-identifiers is that quasi-identifiers cannot be erased as part of the anonymization process since any attribute is potentially a quasi-identifier[411].

An integer, named *k*, is then set. In figure 2 *k* equals 2, which means that the dataset follows *k*-anonymity's requirements if each sequence of values in the quasi-identifier appears at least *k* times-which is 2 in our example[412].

If we observe the chart again, we will notice that the quasi-identifiers "birth=1965" and "gender=m" appear twice; *k*-anonymity is therefore respected. Therefore, a record in the *k*-anonymized data set could not "be mapped back to the corresponding record in the original data set"[413].

In conclusion, this model shows that if there are at least *k* occurrences, the anonymity of a certain dataset is guaranteed[414].

[409] Sweeney. Cit. pg.7.
[410] ENISA. Cit. pg.30.
[411] ENISA. Cit. pg.30.
[412] Sweeney, L. Cit. pg.9.
[413] ENISA. Cit. pg.31.
[414] Sweeney, L. Cit. pg.9.

As we have shown, *k*-anonymity can prevent identity disclosure, since "the *k*-anonymous version of an original record is indistinguishable within a group of *k* records sharing quasi-identifier values"[415].
Nevertheless, *k*-anonymity may not be able to protect attribute disclosure.
This happens for instance when the value of a confidential attribute is the same or nearly the same in all "*k* records sharing the same combination of quasi-identifier values"[416].
After having discussed some existing privacy protection strategies, the following section will proceed offering a conclusion to the Chapter.

3.5 Is it possible to find a balance between regulatory benefits- such as those of smart grids – and privacy protection?

Chapter 3 will end up with a discussion of this open question. Indeed, we firmly believe that the answer should be an affirmative one, but before talking about how to reach this balance, we should focus on its premises.
In other words, if policymakers really aim at finding out a balance representing "a deliberate and thoughtful weighing of regulatory benefits and privacy values", they will first need to "understand the potential environmental benefits" that personal environmental information can involve, as well as their related privacy costs[417].
Potential environmental benefits and privacy costs are context specific variables[418].
In particular, for the first variable, policymakers should understand how access to personal environmental information resulting from AMI technologies could enhance the regulation of environmentally significant behaviours[419].
At the same time, privacy costs related to personal environmental information will be outlined by "considerations specific to the collection and use of the information in support of regulation and, possibly, an evaluation of the value of privacy in environmental information[420]".

[415] ENISA. Cit. pg.31.
[416] Ibid.
[417] Fischer Kuh, K. Cit. pg. 1573.
[418] Ibid.
[419] Ibid.
[420] Ibid.

Some relevant context-specific considerations comprise the type of information that is needed to support regulatory goals, the strategies that need to be carried out to obtain that information, and its ultimate use[421].

On the one hand, as we tried to illustrate, if the value of regulatory benefits of personal environmental information is not sufficiently considered, privacy controls could too greatly and unnecessarily restrict access to information[422].

On the other hand, if privacy harms deriving from the collection of personal environmental information are not enough taken into account, they could even lead consumers to opt out of the use of AMI technologies[423].

Indeed, as we have demonstrated, privacy concerns have certainly been one of the most prominent triggering factors of public backlash opposing AMIs and smart meters' adoption and have in certain cases led municipalities to contrast or even ban their use.

Any regulatory agency should thus outline privacy protection measures "to the level of risk posed by different types of data while maximizing the benefits that disclosure to third parties can offer".

For instance, data can generally be categorized into three types: "customer-specific data containing personally identifying information; customer-specific data stripped of personal identifiers but still indicating usage for single homes; and aggregated data representing neighbourhood- or community-level information[424]".

As third parties increasingly seek access to AMI data, policymakers will need to consider the characteristics of these types of data and categorize regulatory regimes to both maximize AMI benefits and minimize privacy risks.

The effort Regulatory agencies must undertake for setting up regulations concerning AMI data to ensure privacy while furthering important policy and environmental goals is definitely gruelling.

Regulatory policies need indeed to be constantly revised and reviewed since "technologies change, and new concerns arise[425]".

Nevertheless, if we can draw a lesson from these developments is that AMI future, namely its success or failure, depends on customer acceptance.

[421] Fischer Kuh, K. Cit. pp. 1573-1574.
[422] Fischer Kuh, K. Cit. pg. 1574.
[423] Ibid.
[424] J Harvey, S. pg. 2085.
[425] J Harvey, S. pg. 2084.

It is therefore important to create an open dialogue to inform citizens and give voice to their privacy concerns, especially because the shaping of the deployment and use of RFID and smart meter technology is up to them[426].

The purpose of this conclusion is not to criticize the need for privacy protections but to simply underline the importance of finding some trade-offs between access to personal environmental information to support regulation and privacy, as privacy protections are applied to new technologies. For these reasons, according to Justice Stephen Breyer, environmental scholars should open a "national conversation" about how to reach an optimal balance between access to personal environmental information and privacy, so that importance can be attached both to regulatory benefits and those privacy harms associated with access to personal environmental information[427].

[426] J Harvey, S. pg. 2085.
[427] Fischer Kuh, K. Cit. pg.1629.

Chapter 4

Prevailing approaches to privacy policies

This last Chapter sheds light on existing worldwide privacy policies, focusing on the effort institutions have put into the common cause of protecting consumer privacy.
For this purpose, a first glance will be given at the role of the Fair Information Practice Principles (FIPPs) and of the European General Data Protection Regulation, underlining the need to address smart grid challenges at a more technical level, by providing tools and methods aiming at fostering GDPR or FIPPs adherence.
Secondly, Federal Privacy Law and especially The Fourth Amendment and the third party doctrine will be analysed with reference to major legal cases concerning the privacy of those personal information gathered by innovative technologies.
Thirdly, we will describe concrete examples of how American states like Texas, California and Colorado have implemented their own privacy law, apart from federal regulations.
Finally, we will discuss three already implemented techniques to protect privacy in relation to smart-meter or digital-electricity technology.

4.1 Basic privacy principles- the FIPPs, the GPDR and AMI technologies

The 1960s and the 1970s were two important decades for the Federal Constitutional Right to Privacy. It was in this period that most of those privacy principles underpinning privacy policies were articulated for the first time in the United States[428].
The Court held in a series of cases ruling that the Constitution protected a "zone of privacy" with the purpose of safeguarding "individual autonomy in making certain decisions involving their bodies and families"[429].

[428] Lee, D. and J. Hess, D. (2021). *Data privacy and residential smart meters: Comparative analysis and harmonization potential.* Utilities Policy Volume 70. Contents lists available at ScienceDirect Utilities Policy. pg. 2.
[429] J. Solove, D. (2006). *A Brief History of Information Privacy Law* in PROSKAUER ON PRIVACY, PLI. pg. 23.

As far as Information Privacy is concerned, in 1977, the Court held in *Whalen v. Roe* that this "zone of privacy" refers both to "independence in making certain kinds of important decisions"; and to "individual interest in avoiding disclosure of personal matters"[430].

This interest has been precisely defined as the *constitutional right to information privacy,* a right that has been frequently involved in court cases from the 1960s onwards[431].

Nowadays, in all fifty states most of the laws concerning freedom of information find their source in the Freedom of Information Act (FOIA), according to which anyone may request records maintained by an executive agency[432].

In 1973, in line with public privacy concerns about the risks associated with increasing dataset computerization, the United States Department of Health Education and Welfare (HEW) published a report entitled "Records, Computers, and the Rights of Citizens"[433].

The report remarked that individuals were increasingly forced to give up their information "to large and relatively faceless institutions for handling and use by strangers"[434], also specifying that individuals could even not been aware of the fact that their information was being processed by some an organization[435].

For these reasons, the report suggested to adopt a code of "Fair Information Practices"[436].

The Fair Information Practice Principles (FIPPs) are largely recognized principles "agencies use when evaluating information systems, processes, programs, and activities that affect individual privacy"[437] and that should be applied according to the agency's particular mission and privacy program requirements[438].

Among these principles we can cite accountability, authority, minimization, quality and integrity, individual participation, security, and transparency[439]. According to these points, people should be able to find out which of their personal information are in a record and how they are used[440].

---

[430] Ibid.
[431] J. Solove, D. Cit. pg.24.
[432] Ibid.
[433] J. Solove, D. Cit. pg.25.
[434] U.S. Department of Health, Education, and Welfare. (1973). *Records, Computers, and the Rights of Citizens*: Report of the Secretary's Advisory Comm. On Automated Personal Data Systems.
https://www.justice.gov/opcl/docs/rec-com-rights.pdf
[435] Ibid.
[436] J. Solove, D. Cit. pg.25.
[437] Protecting Privacy. Promoting Trust in Government. *Fair Information Practice Principles (FIPPs).*
https://www.fpc.gov/resources/fipps/
[14/10/2022]
[438] Ibid.
[439] Ibid.
[440] J. Solove, D. Cit. pg.25.

In addition, any organization maintaining or sharing records of identifiable personal data must guarantee the reliability of those information for their intended use[441], which must comply with a legally authorized purpose[442].

This entity must also take reasonable precautions to prevent data misuse[443] and guarantee they are maintained for as long as it is necessary to accomplish the purpose[444].

The FIPPs paved the way to privacy laws that developed in the United States during the following decades and influenced privacy law around the world[445].

Some of the fundamental digital privacy rights contained in the FIPPs can be identified in similar forms in one of the major current privacy regulations, namely the European Union's General Data Protection Regulation (GDPR)[446].

Nevertheless, despite the FIPPs and GPDR include some common principles, their policy role is completely different[447].

In the United States, researchers have stated that the "translation of FIPPs into digital privacy law" is confined to the federal-government level[448]. This means that sometimes existing American law proved not to be adequate to take on the challenges posed by high-frequency data transaction[449].

In other words, the FIPPs have been designed for setting up the basis for privacy guidelines and policies, and governments have used them especially in North America, whereas the GDPR is an enforceable legal framework that has not only set guidelines for the collection and processing of personal information but that has also harmonized privacy laws for every European member state[450].

Nevertheless, the GDPR has been criticized too. Although it is considered as a landmark for privacy policy in the world, arguments to cast doubt on the extent to which the GDPR could effectively balance individual privacy rights and collective benefit have been put forward[451].

---

[441] J. Solove, D. Cit. pg.26.
[442] Protecting Privacy. Promoting Trust in Government. *Fair Information Practice Principles (FIPPs).* https://www.fpc.gov/resources/fipps/
[443] J. Solove, D. Cit. pg.26.
[444] Protecting Privacy. Promoting Trust in Government. *Fair Information Practice Principles (FIPPs).* https://www.fpc.gov/resources/fipps/
[445] J. Solove, D. Cit. pg.26.
[446] Lee, D. and J. Hess, D. (2021). *Data privacy and residential smart meters: Comparative analysis and harmonization potential.* Utilities Policy Volume 70**.** Contents lists available at ScienceDirect Utilities Policy. pg. 2.
[447] Ibid.
[448] Ibid.
[449] Ibid.
[450] Ibid.
[451] Ibid.

Another issue concerns how compliance to this regulation is monitored and enforced[452].

Different approaches to the issue were elaborated in Europe.

For instance, in the Netherlands, the Dutch Data Protection Authority brings together privacy complaints consumers send. They can write two types of complaints online: "a possible privacy violation and a complaint regarding personal data processing"[453].

If a problem is detected, the Personal Data Authority needs to reach out the concerned organizations and ask for a change in practices. If repeated violations occur, the case is transferred to the Enforcement Department[454].

In France a Data Protection Agency called "Commission Nationale de I'Informatique et des Libertés" (CNIL) is responsible for ensuring that information technology remains at the service of citizens[455]. This entity helps citizens to be aware of their rights regarding personal data, and it also warns organisations or people who do not comply with the GDPR[456]. Repeated violations can be punished with a penalty up to €20 million and, for companies, it can also correspond to 4 percent of their annual global turnover [457].

In the U.K. a similar role is played by the Information Commissioner's Office (ICO), a non-departmental public body supporting "information rights in the public interest, promoting openness by public bodies and data privacy for individuals".

A similar entity exists in Norway too. Financed by the Norwegian government, the Norwegian Data Protection Authority checks for organizations' compliance with privacy regulations, "provides advice to industry organizations, and receives individuals' complaints"[458].

Another critical aspect researchers have highlighted is how the GDPR should be implemented for AMI technologies[459].

A structural incompatibility between privacy law and smart meters underlies this this problem.

In particular, data protection law explicitly defines what is permitted and what is forbidden according to a specific jurisdiction, whereas in complex information systems such as smart grids,

[452] Lee, D. and J. Hess, D. Cit. pg.7.
[453] Ibid.
[454] Lee, D. and J. Hess, D. Cit. pg.7.
[455] At internet. CLIL.
https://www.atinternet.com/en/glossary/cnil/
[16/10/2022]
[456] Lee, D. and J. Hess, D. Cit. pg.7.
[457] Ibid.
[458] Ibid.
[459] Lee, D. and J. Hess, D. Cit. pg.2.

data flows are processed in different places from all over the world, which means these data virtually run into different national legislations[460].

Moreover, a "legal ex-ante control"- like the one imposed by the GDPR- seems not to be the most suitable solution for cases dealing with the rapid technical development[461].

Several strategies have been proposed to cope with this situation.

Despite self-regulation was listed among the potential solutions, it did not prove adequate in this context. Indeed, it could seem useful to establish that it is not up to a legislator but to involved parties themselves to regulate infringements so that conflicting interest can be resolved [462].

Nevertheless, if actors do not put enough effort or are not enough interested in doing so, this system can easily fail[463].

Another possible solution is that software developers could "decide on the level and content of data protection"[464].

In order to do so, data protection should be simplified and, if we consider the numerous aspects different legal systems share, we could also conclude that similar views on essential data protection elements exist throughout the world[465]. These common views could be gathered to set up a basis for a common *universal* legal framework, even if it seems difficult to identify the most appropriate principles[466].

The purpose should be coming to an agreement to turn abstract principles into formal, technical rules. In this way, we could both make up for the current lack of privacy enforcement and, at the same time, create automated rules allowing software to effectively enforce privacy[467].

Privacy concerns could be resolved generating better regulations via a technical, rule-based enforcement.

However, before creating patterns for concrete rules and strategies to transform generic principles into concrete rules, a selection of the best legitimatised privacy principles should be made.

---

[460] Wagner, A., Speiser, S., Harth, A., Raabe, O., Weis, E. Karlsruhe Institute of Technology. *Basic Privacy Principles for the Smart Grid.*
https://www.w3.org/2010/api-privacy-ws/papers/privacy-ws-20/
[14/10/2022]

[461] Ibid.

[462] Wagner, A., Speiser, S., Harth, A., Raabe, O., Weis, E. Cit.

[463] Ibid.

[464] Ibid.

[465] Ibid.

[466] Ibid.

[467] Ibid.

To that end, one could draw on the European Commission's standard contractual clauses for the transfer of personal data to third European countries, or again find highly legitimized rules in The International Safe Harbor Privacy Principles[468].

Safe Harbor Principles are part of the European Law and were created around the turn of the millennium to protect the digital data of European citizens. They could therefore be a starting point and provide additional material for forming those concrete rules [469].

The European Commission has set up a Smart Grids Task Force, mobilizing a team of five experts (Experts Groups) specialized in different fields[470].

Expert Group 2, is particularly important in our context, since it is in charge of "mitigating the risk on privacy and security of smart metering systems"[471].

The GDPR requires that:

> where a type of processing in particular using new technologies, […] 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 processing operations on the protection of personal data[472].

In response to this article, the Commission worked with Expert Group 2 and issued a draft for carrying out a Data Protection Impact Assessment (DPIA).

In 2017, Guidelines were adopted, enumerating nine criteria establishing the cases when a DPIA should be undertaken[473].

If the processing meets many criteria, then it is more likely it presents a risk to data subjects, and it thus requires a DPIA[474]. Two out of nine criteria are the critical threshold to conduct a DPIA, while for smart meters at least three criteria should be met. Data should undertake an evaluation or scoring process- including profiling and predicting- they should also be processed on a large-scale, and technological or organizational solutions should be applied[475].

---

[468] Ibid.
[469] Techopedia. *Safe Harbor- What Does Safe Harbor Mean?*
https://www.techopedia.com/definition/14227/safe-harbor
[17/10/2022]
[470] Cranium. *Smart Energy and GDPR for utility.*
https://gdpr.be/uncategorized/smart-energy-gdpr-utility/
[17/10/2022]
[471] Ibid.
[472] Intersoft consulting. Art. 35 GDPR- *Data protection impact assessment.*
https://gdpr-info.eu/art-35-gdpr/
[17/10/2022]
[473] Cranium. Cit.
[474] Ibid.
[475] Ibid.

Moreover, the European Commission proposed to make some adjustments to the Electricity Directive so that provisions concerning smart meters' data protection issues could be integrated into the document[476].

Unlike the GDPR -which provides general legal regulations- these proposed modifications for an Electricity Directive would act as *Lex specialis*, namely as law governing a specific subject matter[477].

According to the GDPR, "smart metering deployment and data management have to be settled at Member States' level" but the different roles of the processor and the controller allocated by the GDPR are not explicitly defined at a European level[478].

Apart from the Distribution System Operator, namely those entities responsible for distributing and managing energy from the generation sources to the final consumers[479], some European States have established another entity, called central communication hub[480].

The central communication hub's role is to route the data to the Energy Suppliers, Distribution Systems Operators and other third parties, but all data is stored on the smart meter itself[481].

In conclusion, this paragraph provides an overview of American and European privacy legislation, focusing on the differences between the GDPR and the FIPPs.

We also mentioned the need to create technical rules as a possible means to enforce privacy directly and completely.

The following paragraph will focus on Federal Privacy law, whereas paragraph 4.3 will analyse how some European Members States are building a legal framework for the introduction of smart meters[482].

[476] Ibid.
[477] US Legal. *Lex Specialis Law and Legal Definition.*
https://definitions.uslegal.com/l/lex-specialis/
[17/10/2022]
[478] Cranium. Cit.
[479] Iberdrola. *DSO — how to convert grid management towards a smarter system?*
https://www.iberdrola.com/innovation/distribution-system-operation
[17/10/2022]
[480] Cranium. Cit.
[481] Ibid.
[482] Ibid.

4.2 Federal Privacy Law- The Fourth Amendment and the third-party doctrine

AMI and similar smart grid technologies are promising for our current and future energy and environmental challenges.

Nevertheless, data resulting from smart grids' activity reveal a great amount of information concerning customers' in-home activities, which can lead to legitimate privacy concerns.

As we have already stated, these concerns are particularly deep when data is shared with third parties[483].

If neither statutes nor regulations can provide protection for the privacy of in-home costumers' activities brought up by smart meter data, the Fourth Amendment may offer "some protection, at least against law enforcement's unfettered access to the data"[484].

The Fourth Amendment provides that:

> [t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[485]

This provision aims at safeguarding people's right to privacy and protection from those searches and seizures the law judged "unreasonable"[486]. However, different interpretations have been attached to the adjective "unreasonable"[487].

In 1967 *Katz v. United States* led the court to redefine what constitutes a *search* or *seizure* in the Fourth Amendment to the United States Constitution.

In this prominent case the court determined that what an individual "seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected [488]".

---

[483] J Harvey, S. Cit. pg.2082.
[484] Dancey, B C. (2011). *Privacy Implications of Smart Meters.* 86 Chi-Kent L Rev 161 at 182. pg.183.
[485] Cornell Law School. Legal Information Institute. https://www.law.cornell.edu/wex/fourth_amendment#:~:text=A%20search%20or%20seizure%20is,search%20or%20seizure%20is%20justified. [06/10/2022]
[486] Cornell Law School. Cit.
[487] Dancey, B Cit. pg.183.
[488] National Constitution Center. Supreme Court Case. Katz v. United States. 389 U.S. 347 (1967). https://constitutioncenter.org/the-constitution/supreme-court-case-library/katz-v-united-states#:~:text=.%20.%20.%20.-,%5BT%5Dhe%20Fourth%20Amendment%20protects%20people% [06/10/2022]

With the advent of AMI and similar smart grid technologies challenging cultural privacy norms, the *reasonable expectation of privacy* parameter, referred to as the Katz test, has been cited in thousands of cases.

A reasonable expectation of privacy can arise when "[a] person have exhibited an actual (subjective) expectation of privacy" and "the expectation [is] one that society is prepared to recognize as 'reasonable'[489].'"

In 1979, the Court held that the expectation to keep phone numbers private - when dialled- was not an expectation "that society [was] prepared to recognize as reasonable[490]".

In 1986 the Congress introduced the Pen Register Act, updating The Electronic Communications Privacy Act (ECPA) so that the privacy of outgoing phone numbers could be protected[491].

As technology evolved, law enforcement agencies gained the ability to detect activity within a home by using thermal imaging.

Moreover, since it was ascertained that thermal imaging cameras could be used to view inside a home, in the case *Kyllo v. United States*, the court stated that "monitor heat radiation in or around a person's home, even if conducted from a public vantage point, is unconstitutional without a search warrant[492]".

Indeed, even though the dissent maintained that technology only intercepted heat waves, and therefore no personal information could be inferred, the court rebutted that, on the contrary, a thermal imaging device could disclose intimate details about personal activities, thus violating a reasonable expectation of privacy[493].

If we look closely at these cases, we could infer that the Fourth Amendment would be a deterrent to access by law enforcement to those smart meter data that could potentially divulge intimate information about activities taking place within a customer's house[494].

Nevertheless, no specific privacy policies concerning energy consumption data have been drawn up, neither by the Congress nor by any other federal agency[495] and the United States Supreme Court has

[489] Court Listener.
https://www.courtlistener.com/opinion/107564/katz-v-united-states/summaries/?
[06/10/2022]
[490] Dancey, B C. pg.183.
[491] Ibid.
[492] Justia. US Supreme Court. Kyllo v. United States, 533 U.S. 27 (2001)
https://supreme.justia.com/cases/federal/us/533/27/
[06/10/2022]
[493] Ferguson, A. G. Cit. pg.838.
[494] Dancey, B C. pg.184.
[495] B Klass, A and J Wilson, E. (2014-2015). Energy Consumption Data: The Key to Improved Energy Efficiency. 6 San Diego J Climate & Energy L 69 at 70. pg.86.

not explicitly ruled whether energy consumption data ought to be protected by the Fourth Amendment[496].

A lower court has however established that electricity customers cannot object to install smart meters on Fourth Amendment grounds since, according to the *third party doctrine*, the information a customer transfers to a "business as part of their commercial relationship" is not protected anymore[497].

In the same way, if costumers give up personal data to third parties in exchange for knowing more details about their health, fitness and so on, the third-party doctrine does not provide protection from police requests[498].

Nevertheless, recent cases submitted to the Supreme Court concerning GPS monitoring, have made lawmen wonder whether the third party doctrine should still apply to new digital technologies[499].

As it has been explained before, according to the third-party doctrine "people are not entitled to an expectation of privacy in information they voluntarily provide to third parties" [500].

For instance, if a city would like to find out anyone violating a water conservation ordinance that limits lawn watering to specified times, it could access smart meter data[501].

As a matter of fact, by asking for access to a utility's smart meter records and by using a software to recognize repeated occurrences of a sprinkler's activity at forbidden times, the city would be able to identify those devices which settings are contrary to the ordinance [502].

In doing so, the city would be able to enforce the ordinance in an easy and effective way, using far fewer resources than usual[503].

As a result, "law enforcement is not required to obtain a warrant to access that information", thus government can have access to a great deal of costumers' personal information[504].

Many privacy and technology scholars have criticized this legal provision because of the lack of protection and claim therefore the need to secure customers' data as AMI technologies keep on growing.

The importance attached to the home as "the location afforded the most privacy" in Fourth Amendment, has often been stressed by the Supreme Court[505].

---

[496] Ibid.
[497] B Klass, A and J Wilson, E. Cit. pg.87.
[498] Ferguson, A. G. Cit. pg.843.
[499] B Klass, A and J Wilson, E. Cit. pg.87.
[500] Thompson, R M. II. (2014). *The Fourth Amendment Third-Party Doctrine*. Report. Washington D.C. University of North Texas Libraries, UNT Digital Library. pg.1.
[501] Fischer Kuh, K. Cit. pg. 1624.
[502] Ibid.
[503] Fischer Kuh, K. Cit. pg. 1625.
[504] J Harvey, S. Cit. pg.2082.
[505] Ibid.

This element along with in-home information that AMI data offer, could grind the third-party doctrine application to a halt when dealing with cases concerning smart meters or AMI data[506].

Furthermore, Fourth Amendment protections applies to searches conducted in suspects' homes for the sake of supporting noncriminal administrative regulations[507].

A warrant is needed to carry out this common law enforcement technique, even though in some cases the required conditions are not so stringent[508].

In particular, the government can obtain a warrant to inspect a certain home without any "specific knowledge of the condition of the particular dwelling[509]", it only needs to ascertain that "reasonable legislative or administrative standards for conducting an area inspection are satisfied with respect to a particular dwelling [510]".

Among the factors determining whether these relaxed conditions can be applied to the issuance of a warrant, the degree of importance given to that inspection should be considered, as well as the possible "long history of judicial and public acceptance" of that type of inspection, whether the regulation at issue could feasibly be enforced without area inspections, and to what degree that inspection could invade privacy[511].

If the government decides to collect information to support the regulation of environmentally significant individual behaviours, it may therefore need a warrant even though it could do so upon a relaxed showing[512].

The main issue is that, if the government was required to obtain a warrant even under the less demanding standards, for instance in the context of utility smart meter records, this could pose a significant administrative burden[513].

If we consider the regulation of individuals' behaviour for example, this burden could prove so great as to compromise the regulation's utility. Indeed, as explained in the first Chapter, regulating millions of individuals is far more difficult and administratively heavy than regulating a smaller quantity of industries as source of pollution[514].

---

[506] J Harvey, S. Cit. pg.2083.
[507] Fischer Kuh, K. Cit. pg.1623.
[508] Ibid.
[509] Ibid.
[510] OLR Research Report. (1999). *Searches by administrative agencies.* https://www.cga.ct.gov/PS99/rpt%5Colr%5Chtm/99-R-0265.htm [11/10/2022]
[511] Fischer Kuh, K. Cit. pg.1623.
[512] Ibid.
[513] Fischer Kuh, K. Cit. pg.1623.
[514] Fischer Kuh, K. Cit. pg. 1628.

This aspect has long been regarded as an obstacle to "regulating environmentally significant individual behaviours, in particular with respect to the enforcement of mandates on individuals"[515].
Moreover, some state courts have judged that electric records do not reveal discrete information, thus do not violate privacy.
For example, in *State v. Kluss,* the court ruled there was "no reasonable expectation of privacy in power records under State Constitution"[516]. According to the court, the power records as opposed to telephone or bank ones, do not reveal information about activities taking place within the home of the defendant. Different factors may cause a high-power usage: "hot tubs, arc welders, poor insulation, ceramic or pottery kilns, or indoor gardening under artificial lights"[517].
With the spread of smart meters and of home Electronic Manufacturing Services (EMS) -being these services providing a connection between smart meters and smart appliances- one could predict that society will be increasingly more inclined to consider it is unreasonable to expect that electricity consuming in-home activities would remain private[518].
Let's consider for example that the police need to investigate a suspected drug dealer.
Traditionally they would use surveillance cameras, or they would set up a series of stakeouts or observation posts[519]. However, thanks to the Internet of Things, police can monitor IoT devices and not only know if a suspect is home or not, but also keep track of the activities he or she is doing at home. In this case, one could ask whether obtaining that information constitutes a "search for Fourth Amendment purposes, which, in tum, requires asking whether police obtained the information through physical intrusion-trespass or by violating a reasonable expectation of privacy (Kats test)"[520].
Since the Fourth Amendment protects houses and effects, whenever police enter the suspect's house without a warrant, and undertakes a physical search to view the appliance device meant as a physical object, a clear Fourth Amendment search would take place[521].
In addition, if police touch the IoT device to download data, we will have "a trespass to the expectation of privacy", being the "physical object and its data protected by both the houses and effects language of the Fourth Amendment"[522].

[515] Ibid.
[516] Casetext. *State v. Kluss.*
https://casetext.com/case/state-v-kluss
[11/10/2022]
[517] Fischer Kuh, K. Cit. pg. 1627.
[518] Dancey, B Cit. pg.184.
[519] Ferguson, A. G. Cit. pg.836.
[520] Ferguson, A. G. Cit. pg.836-837.
[521] Ferguson, A. G. Cit. pg.837.
[522] Ibid.

But what would happen if police used a device capable of intercepting—from outside the home—the wireless signals emanating from IoT devices within the suspect's home?

Police would not concretely touch the object, nor it would have access to the data stored on the device; they would however gather "the wireless data as it leaves the house and connects to an outside sensor"[523].

The proposed question is not simple to answer, since if we consider the *physical intrusion-trespass* analysis, there could be no Fourth Amendment search, as no physical invasion of physical property would take place[524].

Nevertheless, this collection of information extracted from inside the house can be approximately compared to *Kyllo v. United States*' case, where it was deemed the defendant's information had to be safeguarded as it came from inside Kyllo's house.

Another similar conclusion was reached in *Jardines v. Florida*. In this case, agents suspected that Mr. Jardines was growing marijuana in his home thus approached his home with a drug-sniffing dog to check whether marijuana was effectively in his home[525]. The dog's alert allowed police to obtain a warrant and after the search Mr. Jardines was charged with trafficking in cannabis[526].

However, the Court stated that "[…] when it comes to the Fourth Amendment, the home is first among equals" and hold that the area "immediately surrounding and associated with the home", also known as the curtilage, must be regarded as "part of the home itself for Fourth Amendment purposes"[527].

Indeed, the dog search was deemed unlawful since it was conducted through the unlicensed physical intrusion onto Mr. Jardines' curtilage[528]. Thus, Justices confirmed "the use of a drug-sniffing dog directed at scents coming from the house violated an expectation of privacy"[529].

Since IoT communication signals originate from the home, they should likewise be protected by the Fourth Amendment[530].

Indeed, according to the Fourth Amendment, an individual ought to have the right to "retreat into his own home and there be free from unreasonable governmental intrusion"[531].

---

[523] Ferguson, A. G. Cit. pp.837-838.
[524] Ferguson, A. G. Cit. pg.838.
[525] Sheppard, White, Kachergus, DeMaggio P.A. *Search and Seizure: Expectation of Privacy and the Physical Intrusion Test.* https://www.sheppardwhite.com/blog/2013/07/search-and-seizure-expectation-of-privacy-and-the-physical-intrusion-test/ [11/10/2022]
[526] Ibid.
[527] Ibid.
[528] Sheppard, White, Kachergus, DeMaggio P.A. Cit.
[529] Ferguson, A. G. Cit. pg.838.
[530] Ibid.
[531] LexisNexis. *Silverman v. United States - 365 U.S. 505, 81 S. Ct. 679 (1961).* https://www.lexisnexis.com/community/casebrief/p/casebrief-silverman-v-united-states [11/10/2022]

Logically, at least for investigations targeting at a specific home, secured communication signals emanating from smart devices within that home would be protected under a reasonable expectation of privacy point of view[532].

Nevertheless, since the concrete act of obtaining these signals do not constitute a physical invasion, except for Kyllo, the Supreme Court has not yet considered whether "individuals have a reasonable expectation of privacy in such signals detailing home appliance usage outside the home"[533].

Anyway, one could suggest this kind of information unveils far more private information than Katz's phone conversation for which police would need a warrant, but the main issue here is that under the actual constitutional law there is no specific protection for IoT data and consequently third-party doctrine rules would be applied[534].

For instance, if police need to keep a house monitored using IoT devices, they could simply request and get those data from the service provider, without having to deal with any Fourth Amendment objection[535].

In *United States v. Jones*, Justice Sotomayor declared the classic third-party doctrine rule had never been absolute and may no longer apply[536].

This legal discourse was carried out in *Carpenter v. United States* too. In 2018, however, the Supreme Court established the government was obliged to obtain a warrant for gaining access to historical cell-site location information (CSLI) but decided not to apply the same requirement to "other, similar types of location-based tracking data maintained by many third parties"[537].

Indeed, Fourth Amendment privacy protections were not extended to all those innovative forms of real time data generated by smart meters or tracking technologies[538].

This case could be the right occasion for the Court to make a change and restrict the scope of the third-party doctrine, but it turned out to be useful only for dealing with CSLI, "leaving the private information potentially exposed to warrantless searches by the government"[539].

---

[532] Ferguson, A. G. Cit. pg.839.
[533] Ibid.
[534] Ibid.
[535] Ferguson, A. G. Cit. pg.840.
[536] Lawfare. *Third-Party Party-Crashing? The Fate of the Third-Party Doctrine.* https://www.lawfareblog.com/third-party-party-crashing-fate-third-party-doctrine [11/10/2022]
[537] Bass, S. (2020). *The Outdated Third-Party Doctrine and the Need for Modernization*, 65 N.Y.L. SCH. L. REV. 259. pg.261.
[538] Ibid.
[539] Ibid.

In short, although scholars expressed their discontent regarding the application of the third-party doctrine, and Justice Sotomayor clearly stated both her deep concern and her associated interest in revisiting its application, the third-party doctrine continues to be traditionally applied[540].

Two model regulations that were adopted even before the advent of smart meters, but that were able to provide a "helpful blueprint for regulators to follow" for the sake of balancing consumer privacy concerns against the needs of law enforcement are the California Public Utilities Commission (CPUC) and the Vermont Law School Institute for Energy and the Environment policies[541].

The CPUC policies were expressly elaborated to "address the issue of law enforcement access to customer utility information"[542].

In 1990 the CPUC first provided an official ban for utilities to release customer-specific information to law enforcement agencies if not in possession of a subpoena or warrant[543].

The Vermont Law School Institute for Energy and the Environment have likewise developed a set of model smart grid data privacy policies offering protection other than those privacy warranties promised by the Fourth Amendment[544].

These policies are valid examples of how to address privacy concerns presented by AMI data, adopting clear guidelines to be must followed for obtaining access to customer information[545].

Even though the Fourth Amendment does not provide security to smart meter data, the Stored Communications Act (SCA), the Computer Fraud and Abuse Act (CFAA), and the Electronic Communications Privacy Act (ECPA) exist so that energy consumption data can be safeguarded from unauthorized disclosure or access[546].

Procedures under the SCA, ECPA, and the Foreign Intelligence Surveillance Act (FISA), require law enforcement to meet some limiting conditions for gaining access to smart meter data for investigative purposes[547].

We have thus demonstrated that some existing federal regulations are likely to promote a better collection and use of energy consumption data for energy efficiency purposes, but other general federal privacy laws may cause customers to oppose extensive third-party access to such data[548].

---

[540] Ferguson, A. G. Cit. pg.840.
[541] Ibid.
[542] Ibid.
[543] Ibid.
[544] Ibid.
[545] Ibid.
[546] B Klass, A and J Wilson, E. Cit. pg.88.
[547] B Klass, A and J Wilson, E. Cit. pg.88.
[548] Ibid.

As smart grids continue to develop, some states, local governments, and utilities have issued more specific policies ruling "the use, aggregation, and sharing of energy consumption data"[549].
The next section will explore some of these policies[550].
To conclude, this part also focused on how courts have questioned the meaning and scope of the third party doctrine, which restrictions could notably increase the administrative burdens related to the use of technology to "help detect, implement, or enforce the regulation of some environmentally significant individual behaviours"[551].
Nonetheless, a desire to protect privacy when dealing with today's digital technologies may be influencing the development of Fourth Amendment doctrine, which could evolve in a way to prevent government from having direct access to information generated by those technologies[552].
Furthermore, considering these technologies often transmit a great deal of information to third parties, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information which are voluntarily disclosed to third parties[553].
The greater visibility afforded to in-home behaviours by smart meter data could lead some state courts to revisit reliance on the third party doctrine and it seems possible the Fourth Amendment may evolve to limit the scope of the third party doctrine in part, to prevent privacy intrusions[554].

4.3 Additional privacy protections beyond general privacy principles and federal law

Besides the general privacy principles of the FIPPs, some American governments have set up different policies frameworks for the implementation of privacy principles with reference to data collection and use from electricity customer data, specifically in the context of AMIs[555].
The smart meter opt-out, opt-in for demand-management programs and associated data sharing, independent data storage and implementation of rules for data sharing and separate monitoring, and the establishment of enforcement agencies, are four recurring practices related to residential smart meters arising in this context[556].

[549] Ibid.
[550] B Klass, A and J Wilson, E. Cit. pg.88.
[551] Fischer Kuh, K. Cit. pg.1622.
[552] Ibid.
[553] Fischer Kuh, K. Cit. pg. 1626.
[554] Fischer Kuh, K. Cit. pg. 1627.
[555] Lee, D. and J. Hess, D. Cit. pg. 7.
[556] Lee, D. and J. Hess, D. Cit. pp.7-8.

Although we will briefly discuss these practices in the following paragraph, we would like to focus now on the first one.

As explained above, opt-out policies are generally implemented whenever a public opposition to smart-meter deployment exists[557].

This means that it may not be always necessary to put this policy in practice; a key factor for utilities is deciding according to the level of public demand for an opt-out policy[558].

The percentage of people deciding to opt out is nonetheless low, and this allows the utility to have "robust demand-management programs" despite the tiny percentage of opt outs[559].

However, contrary to what one might think, privacy concerns are just one factor leading to an opt-out policy. Studies have indeed demonstrated that the among the reasons causing public support for an opt-out policy there could be concerns related to health, hacking, costs, non-functioning meters, or a possible interference with other wireless systems[560].

Another major motivation is obviously public awareness of data breaches, which can also involve electricity consumption data and affect even systems with apparently high data security systems.

In short, opt-out practices could be a valid solution to the challenge posed by public opposition to any "highly granular data collection that can identify daily routines and appliance use"[561].

Even though it is not easy to find out a compromise between costumers' and utilities' interests, it would be useful for countries which have to face this challenge to implement an opt-out approach, taking a cue from similar successful models which are already effective in other countries[562];

4.3.1 How strong privacy laws on smart meters can lead to an increase in smart meters installation- Texas's *Utility Code*

Believing the availability of interval consumption data for all customers could both benefit electricity services and give a boost to customer service innovation, the Texas legislature authorized the accelerated roll-out of advanced meter infrastructure in 2005[563].

[557] Lee, D. and J. Hess, D. Cit.pg. 5.
[558] Lee, D. and J. Hess, D. Cit. pg. 7.
[559] Ibid.
[560] Lee, D. and J. Hess, D. Cit. pg. 7.
[561] Ibid.
[562] Ibid.
[563] King, K., P.E., CEO, SPEER, Bevill, R., Policy Manager. (2016). *Improving access to smart meter data in Texas.* Speer. The South-central Partnership for Energy Efficiency as a Resource. pg.3.

As a consequence, today it is common for customers to use cloud-based digital services to understand and check their energy use, "respond to prices, optimize comfort and cost, or even contribute to reliable operation of the grid"[564].

Service providers can access meter data to detect and try to solve "building or systems problems more quickly, identify maintenance needs, or properly size new equipment installations"[565].

Customers can monitor their electric consumption data thanks to Smart Meter Texas (SMT), namely a website that is owned by the utilities and through which competitive energy services providers (CSPs) can access the data stream[566]. All this is carried out to provide additional data-driven services to customers but can be achieved just if customers give permission to the CSPs[567].

Costumers trust this system because of the *right to privacy of customer consumption information* for all retail utility customers[568].

This right has been formulated in reaction to the common concern that third parties, including potential criminals, could exploit AMI data to figure out whether a residence was occupied, how many individuals were inside at a certain time, and which daily schedules and activities concerned costumers had[569].

Other rules protecting energy consumption data and preventing utilities from selling or disclosing information from advanced metering systems are formulated in an Order issued in 2014 by the Texas Public Utilities Commission[570].

The § 25.44 of the Public Utility Regulatory Act states:

> "[a]n electric utility shall not sell, share, or disclose information generated, provided, or otherwise collected from an advanced metering system or meter information network, including energy consumption data, with an exception for third parties affiliated or contracted with the utility and using that information for customer approved services.[571]"

§ 25.500 introduces a similar disposition: it affirms that utilities "shall not sell, share, or disclose information generated, provided, or otherwise collected from an advanced metering system or meter information network" if customers did not authorize all these activities[572].

[564] Ibid.
[565] Ibid.
[566] Ibid.
[567] Ibid.
[568] B Klass, A and J Wilson, E. Cit. pg.89.
[569] B Klass, A and J Wilson, E. Cit. pg.89.
[570] B Klass, A and J Wilson, E. Cit. pg.97.
[571] Ibid.
[572] B Klass, A and J Wilson, E. Cit. pg.98.

Even though these provisions determine customer consent is a compulsory element for disclosing energy consumption data to third parties, when utilities are creating energy efficiency or demand response programs, they can avoid this obligation and release the information to third parties[573].
Nevertheless, according to the Texas Utility Code:

"[a]ll meter data, including all data generated, provided, or otherwise made available, by advanced meters and meter information networks, shall belong to a customer, including data used to calculate charges for service, historical load data, and any other proprietary customer information[574]"

The Texas Utility Code limits customer information disclosure and affirms customers should dispose of the property of their own information[575]. This means that customers can allow utilities to give that information to third parties when needed, especially if they are assisting the utility in providing service[576].
On the contrary, some utilities maintain that they should have "at least some ownership rights in the data"[577]. According to the National Institute of Standards and Technology (NIST) all data generated by the smart meters constitute a utilities' possession just like data related to car rentals for a car rental company[578]. Moreover, NIST states that if we had to consider smart meter data as a costumer's possession, problems concerning who should be regarded as the true consumer may occur[579]. For instance, both the homeowner and the person renting that same home could claim ownership of the concerned energy usage data[580].
Nevertheless, the strong protections we have pointed out resulted in "the highest penetration of smart meters installation in the country, with more than 86 percent of households having smart meters"[581].
We have already discussed how privacy groups have taken legal actions suing cities that have required smart meter installation and asking courts to slow smart meters' deployment.
Therefore, it is not a coincidence that states with the highest penetration of smart meter installations also have the strongest privacy laws governing them[582].

[573] Vergason, D. Cit. pg.574.
[574] Vergason, D. Cit. pg.558.
[575] Vergason, D. Cit. pg.574.
[576] Vergason, D. Cit. pg.574.
[577] Dancey, B C. Cit. pg.173.
[578] Ibid.
[579] Ibid.
[580] Ibid.
[581] Vergason, D. Cit. pg.558.
[582] Ibid.

Shortly, if states offer effective privacy protections to consumers, privacy advocacy groups will have no reason to hinder smart meter development, thus, as Texas' example demonstrates, smart meter installation will not be hindered.

4.3.2 The "*opt-out*" policy and data privacy rules- California and Colorado

As described at the beginning of the paragraph, opt-out policies are a valid option some state public utility commissions adopt to meet customers' wish to decline the installation or operation of smart meter devices[583].

If customer's denial of smart meter devices becomes a widespread practice, it may not only prevent the collection of personal environmental information, thus hindering all the associated efforts to regulate environmentally significant individual behaviours, but also indirectly raise the costs of smart meter deployment[584].

For instance, in California, privacy groups have pushed four counties and a great number of cities- whose inhabitants constitutes a sizable amount of California's population- to enact a complete ban on all smart meter installations[585].

Consequently, California's Public Utility Commission (CPUC) has adopted opt-out plans to give customers the chance to choose and try to safeguard smart meters development.

In May 2014, the CPUC issued an Order called "Decision Adopting Rules to Provide Access to Energy Usage and Usage-Related Data While Protecting Privacy of Personal Data."

These set of rules created categories of protection differentiating on the bases of which entity was seeking the data and the character of the data in question.

Moreover, different rules for energy consumption data were conferred according to which entity was seeking those data- e.g., local governments, building owners seeking building energy usage data, researchers, and other third parties, like solar photovoltaic installer[586].

This order provided that whenever a third party wishes to access energy consumption data, it requires "the consent of the person to whom the usage or usage-related data pertains", although aggregated data with no personally identifiable information (PII) can be transferred to any party even without customer consent[587].

[583] Fischer Kuh, K. Cit. pg.1616.
[584] Fischer Kuh, K. Cit. pg.1617.
[585] Vergason, D. Cit. pg.558.
[586] B Klass, A and J Wilson, E. Cit. pg.94.
[587] B Klass, A and J Wilson, E. Cit. pg.94.

The PUC also gave life to the Energy Data Access Committee (EDAC) which acts as an "informal body to review disputes between utilities and requesting parties" as well as a forum for updating protocols according to changing technological techniques[588].

Moreover, in a 2014 decision, the Commission discussed the potential for creating an "Energy Data Center", which was consistent with some observations presented in a 2012 briefing paper[589].

As a matter of fact, as early as 2012, the PUC analysed challenges for accessing aggregated data and concluded that "consolidating that information in one location, such as a data center, [c]ould help improve state energy policies and create new market opportunities to save energy"[590].

An "Energy Data Center" would be used to gather and store some level of aggregated energy consumption data, so that personal information could be protected and easily handed over from utilities to third parties- such as governmental entities[591].

In 2014 the PUC established it was not yet time to create an Energy Data Center but decided to study the issue in subsequent agency proceedings [592].

Colorado was the first State in the United States where a Public Utility Commission adopted a "firm rule of customer aggregation to address privacy issues associated with energy consumption data"[593].

In 2012 Colorado Public Utility Commission (COPUC) enacted the "15/15 Rule". This provision is based on a 1997's ruling of the California Public Utilities Commission that was later applied to generic aggregated data access[594].

Specifically, the "15/15 Rule" established a privacy standard for utilities customer anonymity for energy data that could be released to third parties without customer consent[595].

According to this privacy standard aggregated data must include a minimum of 15 customers and within any customer class, "no single customer's data may comprise 15 percent or more of the data aggregated in the report"[596].

---

[588] California. Public Utilities Commission. *Energy Data Access Committee (EDAC).* https://www.cpuc.ca.gov/industries-and-topics/electrical-energy/demand-side-management/energy-efficiency/energy-data-access-committee
[23/10/2022]

[589] B Klass, A and J Wilson, E. Cit. pg.96.

[590] Ibid.

[591] Ibid.

[592] B Klass, A and J Wilson, E. Cit. pg.96.

[593] B Klass, A and J Wilson, E. Cit. pg.93.

[594] Elevate Energy. Smarter energy use for all. *Aggregated Data Access: The 15/15 Rule in Illinois and Beyond.* https://elevatenp.org/wp-content/uploads/1515-Rule-Factsheet-FINAL.pdf
[23/10/2022]

[595] Ibid.

[596] B Klass, A and J Wilson, E. Cit. pg.93.

Even if Colorado undertook to set up this program for third party access to energy consumption data, the way aggregate data are transmitted from utilities to public entities has been criticized and often judged as slow and inadequate[597].

As far as energy usage information ownership is concerned, the Public Service Company of Colorado- an operating utility providing electricity and gas- states that "the energy usage information should be viewed as the property of the utility". It also affirmed that it is up to the COPUC to provide for a mechanism through which utilities can recover "the costs associated with disclosure of customer data to third parties upon the customer's written request"[598].

On the other hand, California's Public Utility Commission considers that customers have the right to decide if they want to release their smart meter data to a third party[599].

Nevertheless, utilities in this case must make some considerations, assessing whether it is more convenient for them to "retain an old analogue meter or to have substantial limitations" imposed on data collection from digital meters. Examples could be holding a smart meter that must be read monthly by an expert or again a smart meter that sends information just at a specific time interval of a certain duration- e.g., one month[600].

Indeed, the opt-out program allows customers to retain a similar meter or continue to use a digital one but with remote communication disabled[601].

In Norway it is compulsory to install smart meters and in France it is up to courts to decide whether a smart meter can be removed. On the contrary, the right to opt out of a smart meter installation is already established in the Canadian provinces of British Columbia and Quebec, in the Netherlands, in the UK, and in some American states, such as California.

As stated before in the paragraph, since an opt-out practice does not allow within-day, time-of-use data to be collected, it can turn out to be a practical tool for increasing customers' trust in relatively efficient privacy protection systems[602].

However, it is important to highlight that the opt-out strategy usually creates a negative marginal cost for the utility[603].

[597] B Klass, A and J Wilson, E. Cit. pg.94.
[598] Dancey, B C. Cit. pg.173.
[599] Ibid.
[600] Lee, D. and J. Hess, D. Cit. pg.5.
[601] Ibid.
[602] Ibid.
[603] Ibid.

If the percentage of people deciding to opt out is high, the utility may incur significant revenue loss and could also lose "grid-stabilization benefits from programs such as load management, time-of-use pricing, and transactive energy"[604].

In addition, since the smart meter needs to be read monthly, the utility must pay a service representative to do that, and it could not generally access all the information that would be helpful during a power outage[605].

Thus, opt-out policies may be a useful practice to at least in part appease privacy concerns.

Nevertheless, a good policy should also consider utilities' point of view and the challenges they must face because of customers opt-outs.

Utilities have therefore sought approval for applying a reasonable charge whenever a customer decides to opt out, but no agreement was reached concerning the amount of this reasonable charge[606].

As more and more utilities started to deploy AMI technologies, legislation to implement state-wide policies have been increasingly adopted[607].

California's state policy, for example, has also authorized to set-up fees and monthly charges for customers who opt out. In general, a one-time fee of $75 and a monthly fee of $10 must be paid by citizens deciding to opt out, except for income-qualified customers who need to pay a one-time fee dropping to $10, and a $5 monthly fee[608].

To date, in two American states, namely New Hampshire and Vermont, customers can opt out from smart meters without having to pay a fee[609].

In a February 2019 decision, the Iowa Utilities Board established that Interstate Power and Light's residential customers could freely decide to opt out without having to pay any additional charge. However, in this decision nothing precludes "interstate or any other utility from submitting opt-out fee proposals for future consideration"[610].

In 2016, a bill in New Hampshire could have overturned the state's opt-in policy by giving utilities the possibility to assess a surcharge on opt-out customers. Even if the bill was not approved, the fact that it had at least been proposed proves that the "state's earlier decision to allow customers to freely decline smart meter installation is not without its critics"[611].

---

[604] Ibid.
[605] Ibid.
[606] Lee, D. and J. Hess, D. Cit. pg.5.
[607] NCSL. Shea, D. and Bell, K. (2019). *Smart Meter Opt-Out Policies.* https://www.ncsl.org/research/energy/smart-meter-opt-out-policies.aspx [23/10/2022]
[608] Ibid.
[609] Ibid.
[610] Ibid.
[611] Ibid.

Supporters maintain that opt-out practices are likely to fade because smart meter installation would become more common, thus making customers more at their ease and familiar with this technology. Until that time, however, states will continue to consider opt-out policies to provide greater customer choice[612].

In conclusion, it is not easy to find a balance between customer's right to opt out and the utility's need to recover for the loss of benefits resulting from the exercise of the customer's right, especially because the widespread use of the smart meter and AMIs does not only benefit utilities, but also produce general benefits of sustainability and resilience[613].

Researchers believe that although a potential for international harmonization at the level of general guidelines and principles exists, the balance in this case would need to be determined by national or subnational energy jurisdictions, always taking into account local perspectives[614].

4.4 Other practices governments have developed both in Europe and in North America to protect privacy with respect to smart-meter or digital-electricity technology

We will finish this Chapter describing some practices that have been implemented respectively in Ontario (Canada), the U.K. and Germany.

Ontario's Privacy Commissioner Ann Cavoukian has been a leading figure in the field of privacy for the smart grid. She is indeed recognised as one of the world's major privacy experts for creating Privacy by Design, a framework which purpose is to "proactively embed privacy into the design specifications of information technologies, networked infrastructure and business practices, thereby achieving the strongest protection possible"[615].

In 2010, International Privacy Regulators passed a Resolution identifying Privacy by Design as an International Standard and eight years after this framework was integrated in the GDPR[616].

[612] Ibid.
[613] Lee, D. and J. Hess, D. Cit. pg.5.
[614] Lee, D. and J. Hess, D. Cit. pg.6.
[615] Ubisecure. (2022). *Privacy by Design, with Ann Cavoukian, Global Privacy and Security by Design Centre.* https://www.ubisecure.com/podcast/privacy-by-design-ann-cavoukian/ [27/10/2022]
[616] Ibid.

At the core of privacy by design is the theory that policies alone cannot guarantee privacy enforcement. On the contrary, privacy should become part of an organization working management system, thus it would not impose a trade-off on utility but an additional utility instead[617].

Researchers have remarked some prevailing practices governments started to adopt both in Europe and North America.

Norway, the UK, and Ontario, for instance, have established an independent data storage system[618].

The independent electricity system operator (IESO) of Ontario operates an independent "Meter Data Management and Repository" (MDMR) for all local electricity distribution system operators (DSOs). MDMR accounts for the collection, management and storage of information related to consumers' consumption metering or electricity use in Ontario.

This repository allows authorized entities, such as service providers, to access the data they respectively require. However, since authorized utility companies can still access plain data and do not employ privacy-preserving protocols, this system can still be improved[619].

In the UK, the Department of Energy and Climate Change (DECC) aims at creating a nationwide data and communications company (DCC)[620]. In other words, this entity would serve as "a central node for all smart metering data from all households in the UK"[621].

Access to customers' measurements would vary according to the type of activity offered by service provider[622]. For basic provisioning with electricity, for example, the service provider would only get monthly readings[623]. If the customer wants, he or she could however give consent to opt in and allow more frequent readings[624].

This approach in is an example of the Privacy first strategy, whereas the one adopted by the IESO in Ontario can be identified as a case of Utility first strategy[625].

To sum up, at this point, several countries have decided to create a separate governmental agency or department that is responsible for supervising privacy-related practices, and that has enforcement authority[626].

[617] Jawurek, M., Góra J. *Privacy in smart grids*. Engineering dissertation. University of Erlangen–Nuremberg. pg.34.
[618] Lee, D. and J. Hess, D. Cit. pg.7.
[619] Jawurek, M., Góra J. Cit. pg.30.
[620] Jawurek, M., Góra J. Cit. pg.30.
[621] Jawurek, M., Góra J. Cit. pg.31.
[622] Ibid.
[623] Ibid.
[624] Ibid.
[625] Jawurek, M., Góra J. Cit. pg.32.
[626] Lee, D. and J. Hess, D. Cit. pg. 8.

Indeed, both the DECC and the IESO, already use or at least envisage to employ "central storage hub for smart metering data"[627].

Nevertheless, it is still unknown whether establishing such a hub could be an effective way to protect all the data that are stored inside, and thus whether "central storage is a good design decision from the standpoint of consumer privacy"[628].

Another common practice is the opt-in for demand-management programs and associated data sharing.

Demand management is a "planning methodology companies use to forecast and plan how to meet demand for services and products". These strategies aim at improving connections between operations and marketing[629].

For instance, real-time pricing, dynamic load management, and transactive energy are all beneficial programs that are based on "highly granular data with high-frequency sampling"[630].

For the purpose of carrying out these programs, utilities or other energy-service providers tend to push customers to enrol, or to opt in, but do not directly oblige them to do so[631].

Utilities generally offer demand management pricing incentives, which can be adapted to local demand to encourage voluntary participation[632]. Some demand response programs consist for example in rewarding large energy consumers that agree to reduce their energy demand during times of electricity grid stress.

Some researchers have indeed explained that specific aggregation rules for data sharing such as the California-based "15/15 Rule", are way too strict under many circumstances and have thus analysed more flexible practices.

One of those practices is the assessment process, which would provide an analysis of the potential risk of privacy breaches within a specific use case for shared data, such as data sharing with owners of properties with multiple units[633].

In the second volume of "Guidelines for Smart Grid Cyber Security", the United States National Institute for Standards and Technology (NIST) have integrated a report called "Vol.2, Privacy and the Smart Grid"[634]. This document introduces United States privacy laws and regulations and wonders

[627] Jawurek, M., Góra J. Cit. pg.33.
[628] Ibid.
[629] Oracle Netsuit. Abby Jenkins. *What Is Demand Management: Functions, Process and Examples*. https://www.netsuite.com/portal/resource/articles/inventory-management/demand-management.shtml [25/10/2022]
[630] Lee, D. and J. Hess, D. Cit. pg. 7.
[631] Ibid.
[632] Lee, D. and J. Hess, D. Cit. pg. 7.
[633] Ibid.
[634] Ibid.

whether they are suitable for smart meters. After illustrating the results of a privacy impact analysis of the smart grid, the report confirms the importance of performing privacy impact assessments and to explicitly develop and document privacy policies[635].
Another practice that has been examined in the United States is based on procedures for sharing health information. In this case it would be up to an expert to assess and remove specified categories of PII, again depending on the use case[636].

The list of practices we have discussed so far is not complete, meaning that other strategies could be developed in the near future[637].
Nevertheless, we agree with those scholars- such as Dasom Lee and David J. Hess- claiming the need for comparative policy research. Indeed, further research towards a cross-cultural consistent approach to digital privacy policy for electricity is needed.

This Chapter tried to introduce a potential common ground for strategies implementing privacy policies and principles for AMIs.
Those common strategies should also be consistent with the privacy provisions comprised in the FIPPs and GDPR and should also help avoid public opposition to AMIs[638].
However, all these goals are not easy to reach. They should be achieved step by step, which require therefore a great effort.
One of these steps concerns system designers' work to implement technologies suitable for different countries, removing "design failures due to unforeseen constraints imposed by differences across countries in privacy rules and regulations"[639].
Finding a perfect equilibrium between AMI technologies' environmental public benefits and individuals privacy takes time, and since data collection and breaches can happen even unbeknownst to stakeholders', governments should continue to establish new guidelines and policies to regulate existing practices through a transparent and accountable decision-making process[640].

[635] Ibid.
[636] Lee, D. and J. Hess, D. Cit. pg. 7.
[637] Lee, D. and J. Hess, D. Cit. pg.8.
[638] Lee, D. and J. Hess, D. Cit. pg. 8.
[639] Ibid.
[640] Ibid.

Conclusion

If the complexity of the environmental realm will not diminish, our capacity to realize and understand how our planet's natural equilibria are changing and to tailor consequent policy responses seems likely to increase rapidly.

Technological advances of the Information Age will make it possible to fill information gaps in problem identification, causal specification, impact evaluation, and policy intervention.

They will give us the chance to make environmental protection more data-driven, empirical, and analytically rigorous, and this will allow a low-cost tracking of pollution and natural resource as well.

The aim of the following thesis work was to demonstrate that smart grid technology and AMI technology can provide a great support for decarbonizing the nation's electric grid.

Allowing to create a reliable grid while offering consumers the possibility to control their electrical usage, these technologies are really proving to be a valid tool for supporting climate action and fostering individual responsibility.

This work also delved into Informational Regulation and Norm Management domain, and after demonstrating how different voluntary standards can be manipulated and used to claim fake adherence to sustainable and ethical principles, it concluded that uniform Standard and Certification Systems should be adopted.

Furthermore, the potentiality of adding the blockchain technology in the certification process was highlighted too.

The blockchain could be a useful tool for keeping track of a companies' production methods and processes, as well as for checking their compliance with recognized standards.

As it has been illustrated so far, this system would both impede the PBC from imposing its own sustainability standards and prevent anticompetitive behaviors, thus creating a reliable certification system.

It will be therefore important to invest both in smart grid's implementation, and in research projects for finding out ways to overcome all the still existing obstacles to blockchain-based certification systems.

However, although AMI deployment is not a new practice, it has been proved that privacy regulations have not kept pace with technological change.

The huge collection of information enabled by the smart grid has the potential to sneak in one of the few remaining spaces of privacy consumers can have today: home.

As discussed in the third Chapter, privacy advocate groups have opposed with zeal the installation of smart meters in their communities, insisting on the great risk to privacy these innovations could lead to.

Yet, the numerous benefits resulting from smart grids and the impact on reducing fossil fuel use are way too significant to restrict its deployment.

Considering all the benefits and advantages these electricity networks can bring to consumers and utilities, legislatures need to update privacy laws or create new strong privacy regulations which would be able to protect them and reflect an appropriate use of smart grid information.

Common basic privacy principles and thus a potential common ground for privacy policies already exist, and some exemplary strategies for implementing privacy protections have already been detected in this context.

As we have shown, the GDPR and the FIPPs provide a set of definitions and principles that are important for the international scenario. These principles need however to be further adapted to AMI technologies' context if we really want to maximize AMI benefits and minimize both privacy risks and customers' diffidence.

Creating laws that protect privacy and give utilities the ability to fully utilize information created by the smart grid requires a difficult but vital balance.

The title of this thesis has indeed been at the centre of all this work; again, if we want to find trade-offs, a dialogue needs to be opened between policymakers, environmental scholars, certification system designers and IoT engineers.

This cooperation may seem utopic but to keep nations' grid strong and continue the decarbonization of our electricity grid, nothing less will do.

New technologies make it possible to fill data gaps in a systematic and sophisticated manner and to respond better to problems that involve multiple variables.

We should therefore take advantage of them, setting up a technical enforcement to ensure compliance with privacy regulations.

RIASSUNTO IN ITALIANO

Il presente lavoro di tesi si è occupato di trattare il ruolo che i Big Data, ed in particolare tecnologie quali smart meters, internet of things, reti di distribuzione intelligenti e smart grids, possono investire nella lotta al cambiamento climatico.

Il lavoro è stato diviso in quattro capitoli. Il primo capitolo, intitolato "Big Data and Climate Change", nel suo primo paragrafo riporta l'attenzione su due accordi internazionali in particolare: la Convenzione di Aarhus e l'accordo di Parigi sui cambiamenti climatici.

La Convenzione di Aarhus fu siglata in Danimarca già nel 1998 ed entrò in vigore nel 2001.

Si tratta per esteso della "Convenzione sull'accesso alle informazioni, la partecipazione dei cittadini e l'accesso alla giustizia in materia ambientale", i cui punti fondamentali furono l'informazione ambientale, la partecipazione del pubblico ai processi decisionali rilevanti per l'ambiente ed infine l'accesso alla giustizia in materia ambientale.

Tale convenzione rivestì una particolare importanza in ambito internazionale, in quanto permise di creare un legame tra protezione ambientale, diritto all'informazione e partecipazione democratica.

Da quel momento, infatti, venne stabilito che il potere pubblico dovesse essere esercitato in modo trasparente ed affidabile e che dovesse inoltre essere accessibile a cittadini ed imprese.

Questo controllo di legalità comportò l'obbligo per i pubblici poteri di fornire adeguate informazioni sull'ambiente e di offrire al pubblico effettive possibilità di partecipare al processo decisionale in materia ambientale. In questo modo la responsabilità e la trasparenza del processo decisionale aumentarono, così come la consapevolezza e il sostegno del pubblico nei confronti delle decisioni adottate.

Un altro notevole passo avanti per la politica internazionale fu la ratifica dell'accordo di Parigi, con cui l'Unione Europea e tutti i suoi Stati membri si impegnarono a portare avanti una strategia a lungo termine per ridurre le emissioni di almeno il 55 percento entro il 2030 rispetto ai livelli del 1990.

Nonostante ciò, alcuni governi europei non sono riusciti a garantire una progettazione e un'attuazione efficace di politiche volte a mitigare la crisi climatica.

Da questo contesto emergono le *climate litigation,* azioni legali avviate con lo scopo di imporre a governi o aziende il rispetto di determinati standard in materia di riduzione delle emissioni di gas ad effetto serra e di limitazione del riscaldamento globale. Si tratta di una pratica sempre più utilizzata e che sta permettendo di lasciare sempre più spazio ad un nuovo diritto ambientale.

In particolare, sono stati analizzati quattro casi in cui i tribunali nazionali di Paesi Bassi (*Urgenda*), Irlanda (*Friends of the Irish Environment* case), Francia (*Grande-Synthe* case) e Germania (*German*

Climate Protection Act case) hanno obbligato i rispettivi Paesi a ridurre le loro emissioni nazionali complessive.

Tra questi, il caso trainante che ha ispirato azioni legali e sentenze simili, menzioniamo la vicenda che vide contrapporsi i Paesi Bassi e un'organizzazione non governativa chiamata *Urgenda.*

Con l'appoggio di centinaia di cittadini, quest'ultima riuscì a trionfare in ogni grado di giudizio, fino alla Corte suprema che nel 2019 condannò lo Stato ad abbattere le proprie emissioni di gas ad effetto serra.

Il primo capitolo prosegue poi spostando il focus della responsabilità ambientale sui singoli individui, spiegando che la percezione errata che essi possiedono del loro impatto ambientale è uno dei principali fattori che fa sì che questi non adottino un comportamento responsabile nei confronti dell'ambiente.

È stato provato infatti che singoli individui tendono a considerare minimo, e quindi generalmente insignificante, il loro apporto all'inquinamento ambientale.

Al contrario, ciascun individuo inquina con quantità spesso invisibili quando rilasciate nell'ambiente, ma il cui impatto diventa importante quando queste fonti di inquinamento si sommano a quelle di altri individui col tempo.

Il focus è stato successivamente spostato sul diverso approccio normativo che caratterizza l'entità "individuo" e la fabbrica, agente inquinante per eccellenza. Gli individui sono infatti di gran lunga più numerosi e dispersi, ed è più probabile che reagiscano in modo diverso all'intervento normativo e agli sforzi del governo per controllare i loro comportamenti, opponendosi all'intrusione di quest'ultimo. È per questo motivo che la legge e la politica ambientale dovrebbero essere adattate per affrontare meglio e più direttamente il comportamento individuale rispetto a quello delle grandi fonti industriali di inquinamento.

In questo contesto, la tassonomia di Lawrence Lessig è uno strumento molto utile per capire come un moderno regime normativo possa cercare di regolare il comportamento.

Lawrence Lessig è un giurista americano e professore di diritto alla Harvard Law School, nonché fondatore di Creative Commons, un'organizzazione no-profit che mira ad ampliare la disponibilità e la quota legale delle opere protette da copyright. Lessig distingue quattro vincoli per regolare il comportamento. Questi vincoli sono: la legge (o i mandati), le norme, il mercato e l'architettura.

Mentre le leggi o i mandati impongono dei requisiti al comportamento e prevedono sanzioni in caso di mancato rispetto di questi, le norme regolano il comportamento sia attraverso le aspettative che la comunità impone (norme esterne o sociali) sia attraverso le aspettative degli individui stessi (norme

interne o personali). L'architettura deve essere invece intesa in senso lato, ossia come organizzazione di uno spazio di qualsiasi genere attraverso l'utilizzo dei materiali che si hanno a disposizione.
Si tratterebbe della "natura" di un contesto, ma a differenza del dato naturale l'architettura può essere per lo meno in parte modificata per rivedere l'assetto organizzativo dello spazio in questione.
Ognuna di queste quattro modalità di regolamentazione può aiutare i governi a controllare e regolamentare i comportamenti individuali: direttamente (attraverso mandati) o indirettamente (regolando le norme, il mercato o l'architettura).
Successivamente questo lavoro si è occupato di analizzare la regolamentazione di comportamenti individuali rilevanti dal punto di vista ambientale.
Per riassumere quanto discusso, poiché le persone sono più propense a reagire a ciò che percepiscono come qualcosa che possa avere un impatto diretto su sé stesse (o sui loro discendenti), la loro volontà di agire al di là del presente potrebbe essere incoraggiata integrando le informazioni sul "presente" con quelle sul "futuro". Così facendo, si dovrebbe riconoscere un dovere intergenerazionale, con la consapevolezza che se non si interviene progressivamente a livello locale, e di conseguenza globale, le società future dovranno affrontare un'esistenza che sarà fisicamente e politicamente più precaria.
Un modo per venire meno a questo problema è quello di utilizzare le informazioni ambientali personali generate dalle cosiddette "smart grids", insieme alle informazioni ricavate dai dati aperti di dominio ambientale.
Una smart grid è una rete che integra sia una rete di informazione che una rete di distribuzione elettrica, permettendo lo scambio di informazioni tra produttori e consumatori in modo da gestire in maniera "intelligente" e ottimale domanda e offerta. Grazie a queste reti la produzione e la distribuzione di energia possono essere regolate sulla base dell'energia rinnovabile prodotta e immessa in rete in quel dato momento.
Si tratta di una "rete intelligente" proprio perché questo sistema integrato di informazioni permette di gestire surplus o deficit sulla rete elettrica in maniera flessibile, garantendo un risparmio sui costi e una minore emissione di gas ad effetto serra.
In seguito, una piccola sezione è stata dedicata all'Internet of Things, termine con cui si indica l'estensione della connessione Internet ad oggetti di diverse tipologie, che trasmettono dati in rete senza la necessità che avvenga un'interazione da uomo a uomo o da uomo a computer.
Gli oggetti possono essere così monitorati e gestiti da remoto e sono dotati di identificatori unici (UID).

Al giorno d'oggi le cosiddette “case intelligenti” sono dotate di elettrodomestici o di fonti di risorse energetiche rinnovabili che possono essere considerate tecnologie appartenenti all’Internet of Things, in quanto consentono agli utenti di caricare e scaricare dati e comandi.

Poiché i sette domini già esistenti per il modello concettuale delle smart grids non includono l’Internet of Things, recentemente sono stati fatti molti tentativi per introdurre quest’ultimo come tecnologia abilitante per la rete.

Tre sottoparagrafi di questo lavoro sono stati inoltre dedicati rispettivamente all’RFID, acronimo inglese di Radio Frequency Identification, ad Ambient Orb e al progetto PlanetWatch.

L’RFID è la tecnologia di identificazione automatica basata sulla propagazione nell’aria di onde elettro-magnetiche. Questa tecnologia permette di rilevare a distanza in modo univoco, automatico e massivo, oggetti, animali e persone sia statici che in movimento.

L’RFID funge pertanto da ponte tra mondo fisico e mondo digitale, e viene usato per identificare un prodotto e autenticarlo, seguendolo nelle sue fasi di produzione, distribuzione e consumo oltre che per raccogliere ed intrecciare dati generati da altri attori coinvolti nel processo.

Ambient Orb è invece un esempio di tecnologia creata per favorire il risparmio energetico.

Si tratta di una palla di vetro smerigliato che si illumina assumendo vari colori per segnalare condizioni critiche di picco della domanda sulla rete intelligente. In particolare, si illumina di rosso quando un cliente utilizza molta energia e i prezzi sono più alti, mentre diventa verde quando il consumo di energia è basso. L'intelligenza incorporata di Ambient Orb e la connessione alla rete consentono quindi di produrre un riscontro in merito a quella che è la situazione energetica in tempo reale, fornendo agli utenti informazioni dettagliate sul loro comportamento ecologico ed incoraggiandoli così a fare scelte di consumo energetico più intelligenti.

Infine, PlanetWatch è una startup nata a gennaio 2020 che si occupa di monitorare la qualità dell’aria attraverso una rete globale di sensori.

In breve, sfruttando la blockchain Algorand, il software avanzato di acquisizione dati sviluppato al CERN e sensori di qualità dell'aria sviluppati da un importante istituto di ricerca, PlanetWatch decentralizza, incentiva e rende più competitivo il monitoraggio della qualità dell'aria.

Questa società, inoltre, incoraggia i cittadini a installare i suoi sensori, collaborando con i governi locali per sensibilizzare i cittadini sui problemi della qualità dell'aria e per identificare degli “ambasciatori” il cui obiettivo è quello di reclutare altre persone volenterose di far parte del progetto.

Inoltre, creando soluzioni di purificazione dell'aria e di monitoraggio, PlanetWatch ha colmato una lacuna nel mercato, fornendo proiezioni in tempo reale sui rischi di infezione da COVID-19 attraverso aerosol e verificando la conformità con gli ultimi standard di qualità dell'aria.

Insomma, questa azienda è riuscita a trovare un equilibrio ottimale tra qualità dei dati, tempi di implementazione della rete e costi, fornendo a città, industrie e cittadini informazioni accurate, tempestive e di facile comprensione sulla qualità dell'aria.

Tuttavia, parallelamente a questo crescente interesse per tali innovazioni, la potenziale violazione della privacy dei dati personali dei consumatori che l'uso incrementale dei Big Data può comportare, desta sempre più preoccupazione.

Dopo aver fornito una definizione di privacy, intesa qui come diritto all' autodeterminazione informativa, ovvero il diritto di ogni persona di accedere ai propri dati, quale che sia il soggetto che li detiene e il luogo dove sono conservati, per chiederne l'integrazione, la rettifica, la cancellazione secondo le modalità previste dalla legge, sono stati evidenziati una serie di limiti legati alla raccolta e all'utilizzo di informazioni personali relative alla tecnologia RFID e alle smart grids.

Gli stati possono limitare l'implementazione della tecnologia RFID imponendo condizioni sul suo impiego nelle patenti di guida o in altri documenti di identificazione rilasciati dallo Stato, criminalizzandone l'uso per commettere frodi o furti di identità, o ancora introducendo leggi più generali che vietano il processo che la tecnologia RFID impiega per ottenere informazioni.

Tuttavia, nonostante la risoluzione del 2000 della National Association of Regulatory Utility Commissioners (NARUC) abbia affermato la necessità impellente di adottare delle politiche di controllo della privacy, solo pochi stati in America, come la California, hanno effettivamente iniziato a valutare le questioni di privacy associate alle smart grids.

Un caso che è invece esemplificativo della battaglia in corso in molte parti del Paese contro la diffusione delle smart grids e che ha occupato parte del terzo capitolo è quello di Naperville.

Naperville è una città situata fuori Chicago, nello Stato dell'Illinois, che negli ultimi anni ha assistito a un notevole incremento nell’installazione di smart grids. Questo processo è stato accelerato dall'American Recovery and Reinvestment Act, una decisione adottata nel 2009 dal Dipartimento dell'Energia degli Stati Uniti (DOE) con cui venivano stanziati 3,4 miliardi di dollari da investire in quella che è stata battezzata la “Smart Grid Initiative (NSGI) di Naperville”.

I clienti non potevano rifiutarsi di prendere parte al programma, ma potevano decidere di pagare una tassa una tantum insieme a un’altra mensile, se desideravano disattivare le funzioni di trasmissione del contatore, il che implicava anche una lettura mensile manuale da parte di un dipendente dell'azienda.

Nonostante questo programma mirasse ad aumentare l'efficienza energetica e a ridurre le emissioni, responsabilizzando i consumatori e fornendo loro più strumenti e informazioni per gestire il proprio

consumo e i costi dell'elettricità, alcune persone hanno espresso preoccupazioni in merito alla privacy dei loro dati.

Portavoce di questi timori, un gruppo di cittadini, chiamato Naperville Smart Meter Awareness (NSMA), ha citato la città in giudizio, sostenendo che l'installazione delle smart grids violasse il diritto al Giusto Processo del Quattordicesimo Emendamento, nonché il divieto di perquisizione governativa del Quarto Emendamento e l'Americans with Disabilities Act (ADA)".

Secondo il querelante, le tariffe imposte sarebbero state discriminatorie nei confronti dei residenti disabili, la cui salute sarebbe stata messa a rischio a causa delle interferenze tra le radiazioni a radiofrequenza prodotte per comunicare le informazioni alla società di servizi e i loro dispositivi medici.

La corte respinse sia le richieste relative alla violazione dell'ADA che le restanti.

Nonostante infatti l'utilizzo dei dati potesse essere considerato una perquisizione soggetta ai vincoli del Quarto Emendamento, la Corte ha stabilito che si trattasse di un trasferimento volontario di informazioni a terzi, e che quindi, in quanto tali, queste potessero essere trasferite al governo senza problemi o particolari restrizioni costituzionali.

La Corte Suprema ha pertanto deliberato che i residenti di Naperville, dal momento in cui avevano iniziato a condividere volontariamente i propri dati ed informazioni con la smart grid, avevano rinunciato a qualsiasi aspettativa di privacy nei confronti del trasferimento di dati in questione.

Questa sentenza è solo un esempio dell'incapacità di molti tribunali di venire in contro alle preoccupazioni degli utenti. Di conseguenza, molte comunità americane hanno adottato indipendentemente delle leggi volte a vietare o a rendere facoltativa l'installazione di smart grids.

L'ultima sezione del terzo capitolo, dopo aver delineato la differenza tra quelle che sono state definite le "due generazioni di diritto ambientale" negli Stati Uniti, propone un quadro generale di possibili tecniche di protezione dei dati e approcci per la tutela della privacy nelle smart grids.

La prima generazione di leggi ambientali risale agli anni '70 e si basa su un modello di regolamentazione dall'alto verso il basso definita "command-and-control".

In questo caso, il governo spingeva le aziende a adottare specifiche tecnologie di controllo dell'inquinamento, installando attrezzature apposite e sottostando al pagamento di eventuali sanzioni in caso di mancato rispetto di tali disposizioni.

Nonostante questo modello sia facilmente gestibile e applicabile, nel corso del tempo degli economisti ne hanno evidenziato molti aspetti negativi, appoggiando invece le strategie che fanno parte della cosiddetta "seconda generazione" in materia di protezione ambientale.

I regolamenti di seconda generazione consentono infatti alle industrie di trovare ed implementare i propri approcci, senza dover sottostare a una presunta migliore tecnologia imposta dall'alto.
Gli olandesi sono stati tra i primi ad implementare questo metodo con il loro "Energy Efficiency Benchmarking Covenant", un patto che il governo olandese ha negoziato con alcune associazioni industriali del Paese. Questo accordo prevedeva che le aziende aderenti migliorassero sistematicamente il loro tasso di efficienza energetica per unità di prodotto, e controllassero scrupolosamente il loro utilizzo di energia.
Un'altra iniziativa che si posiziona sulla stessa linea è l'Emergency Planning and Community Right to Know Act (EPCRA). Negli Stati Uniti, infatti, dal 1986 ad oggi, questa legge richiede alle aziende di comunicare la quantità di sostanze chimiche pericolose che rilasciano o trasferiscono in un anno, e raccoglie tutti questi dati in un database disponibile al pubblico chiamato Toxic Release Inventory (TRI). Inoltre, l'EPCRA pubblica un rapporto annuale in cui figurano le aziende che hanno rilasciato il maggior numero di sostanze tossiche.
È stato provato che, grazie al TRI, il rilascio di sostanze tossiche nell'ambiente è notevolmente diminuito. In effetti, se un'azienda dovesse comparire in tale elenco, non solo verrebbe indubbiamente screditata, ma perderebbe anche la fiducia dei consumatori.
Se spostiamo la nostra attenzione sulle questioni relative alla privacy, potremmo fare un parallelismo tra le industrie di cui abbiamo parlato finora e le imprese basate sull'informazione.
Infatti, nessuna azienda vorrebbe essere riconosciuta come un grande inquinatore, ma nemmeno come realtà in cui avvengono frequentemente violazioni della privacy o fuga dei dati.
È stata infatti proposta la creazione di un Data Release Inventory (DRI), un rapporto che funzioni come il TRI e che richieda alle compagnie basate sull'informazione di riferire la quantità di informazioni personali rilasciate annualmente. Questo rapporto dovrebbe anche indicare se la divulgazione dei dati è stata intenzionale o meno, e dovrebbe essere diffuso pubblicamente dai funzionari governativi che, a loro volta, dovrebbero pubblicare una classifica annuale delle prestazioni delle singole aziende.
Riteniamo quindi che, come nel caso del TRI, questa iniziativa possa essere molto utile e possa ben inserirsi tra le strategie di protezione delle informazioni personali.
Successivamente sono state analizzate delle tecniche di anonimizzazione ed in particolare è stato sinteticamente spiegato il funzionamento del modello "K-anonimato".
Il quarto ed ultimo capitolo fa luce sulle politiche relative alla privacy esistenti a livello mondiale, concentrandosi sul ruolo dei Fair Information Practice Principles (FIPP) e del General Data Protection Regulation (GDPR).

Il GDPR è un'unica serie di norme sulla protezione dei dati entrata in vigore nel 2018 e valida per tutte le imprese che operano all'interno dell'Unione Europea. Lo scopo di questo regolamento è quello di garantire alle persone un maggiore controllo sui loro dati personali, così come quello di garantire alle imprese condizioni di parità e uniformità all'interno dell'Unione Europea.
I Fair Information Practice Principles (FIPPs) sono invece dei principi ampiamente riconosciuti che si basano invece sui principi dello U.S Privacy Act del 1974. Secondo i FIPPs i sistemi informativi, i processi, i programmi e le attività che riguardano la privacy dovrebbero essere valutati applicando tutta una serie di principi, tra cui responsabilità, autorità, minimizzazione, qualità e integrità, partecipazione individuale, sicurezza e trasparenza.
Sono state tuttavia riscontrate delle mancanze per quanto concerne questi importanti regolamenti, in particolare in riferimento alla necessità di inserire delle clausole più tecniche, che forniscano strumenti e metodi più specifici alle sfide poste dalle smart grids.
Questo lavoro si è successivamente addentrato nella legge federale americana relativa alla privacy, ed ha in particolare analizzato il Quarto Emendamento e la "third party doctrine", con riferimento a casi legali riguardanti la privacy delle informazioni personali raccolte da nuovi sistemi tecnologici.
In particolare, l'attenzione è stata posta sul modo in cui i tribunali hanno messo in discussione il significato e la portata della "third party doctrine", le cui restrizioni potrebbero tuttavia far aumentare notevolmente gli oneri amministrativi legati all'uso della tecnologia per aiutare a rilevare, attuare o far rispettare la regolamentazione di alcuni comportamenti individuali significativi dal punto di vista ambientale.
Inoltre, è stato evidenziato come il desiderio di proteggere la privacy in questo contesto potrebbe influenzare uno sviluppo della dottrina del Quarto Emendamento, che potrebbe evolversi in modo da impedire al governo di avere accesso diretto alle informazioni generate da tali tecnologie, limitando inoltre la portata della "third party doctrine", e prevenendo così intrusioni nella privacy degli utenti.
Sono stati infine analizzati ulteriori esempi di leggi e regolamentazioni adottati rispettivamente in California, Texas e Colorado, tutti indubbiamente con degli aspetti da migliorare, ma il cui sforzo è comunque degno di nota.
Lo scopo di questo capitolo era dimostrare l'esistenza di potenziali principi comuni per la creazione di strategie e l'attuazione di politiche volte alla protezione della privacy.
Tali strategie dovrebbero essere sviluppate coerentemente con quanto disposto da FIPPs e GDPR e dovrebbero inoltre contribuire a ridurre l'opposizione pubblica nei confronti delle nuove tecnologie in questione.

Il GDPR definisce esplicitamente ciò che è consentito e ciò che è vietato in base a una specifica giurisdizione, mentre in sistemi come quelli delle smart grids, i flussi di dati vengono elaborati in luoghi diversi di tutto il mondo, il che significa che questi dati si scontrano virtualmente con diverse legislazioni nazionali.

Inoltre, un "controllo legale ex-ante", come quello imposto dal GDPR, non sembra essere la soluzione più adatta per i casi che hanno direttamente a che fare con sistemi il cui sviluppo tecnico è rapido e continuo.

Per far fronte a questo problema sono state proposte diverse strategie, tra cui l'opzione di permettere agli sviluppatori di generare delle regole automatizzate che permettano ai software di applicare efficacemente la privacy. Tuttavia, questo necessiterebbe di un insieme di principi semplificati per garantire la privacy, formati dall'unione dei punti che i diversi sistemi giuridici condividono, dando vita così a una base per un quadro giuridico comune "universale". A tal fine si potrebbe attingere per esempio alle clausole contrattuali standard della Commissione europea per il trasferimento di dati personali a paesi terzi, o ancora trovare regole altamente legittimate nei principi internazionali sulla privacy stabiliti dall'accordo "Safe Harbor".

Un accordo di questo calibro potrebbe così permettere di trasformare i principi astratti in regole formali e tecniche, compensando il problema della mancata applicazione e rispetto dei principi a protezione della privacy.

Per riassumere, il perfetto equilibrio tra i benefici ambientali che le tecnologie di cui abbiamo trattato possono apportare, e la salvaguardia della privacy degli utenti è dunque arduo da trovare.

Ritorniamo quindi al punto di partenza, vale a dire al titolo di questa tesi: "*The role of digital technologies on climate protection: privacy costs and trade-offs*".

Al centro di tutto questo lavoro vi è infatti il pensiero secondo cui per raggiungere dei compromessi è necessario aprire un dialogo tra politici, studiosi dell'ambiente, progettisti di sistemi di certificazione e ingegneri IoT.

Questa cooperazione potrà sembrare utopica, ma risulta auspicabile per il potenziamento e la digitalizzazione delle infrastrutture di rete e per una conseguente piena transizione energetica.

Bibliography

Al-Ali, A. and Aburukba, R. (2015). *Role of Internet of Things in the Smart Grid Technology*. Journal of Computer and Communications, 3, 229-233. doi: 10.4236/jcc.2015.35029**.**

Alston, P. and Adelmant, V and Blainey, M. (2021). *Courts, Climate Action and Human Rights: Lessons from the Friends of the Irish Environment v. Ireland Case.* Litigating the Climate Emergency: How Human Rights, Courts and Legal Mobilization Can Bolster Climate Action (Cambridge University Press). Available at: https://ssrn.com/abstract=3855759

Arriba-Sellier, N. (2021). *The Grande Synthe Saga Continues: A Pyrrhic victory for climate litigation?* VerfBlog. Available at: 10.17176/20210704-135842-0

B Klass, A and J Wilson, E. (2014-2015). *Energy Consumption Data: The Key to Improved Energy Efficiency*. 6 San Diego J Climate & Energy L 69 at 70.

Babcock, H M. (2009). *Assuming Personal Responsibility for Improving the Environment: Moving Toward a New Environmental Norm*. Georgetown Law Faculty Publications and Other Works.

Backes, C.W., van der Veen, G.A. (2020). *Urgenda: the final judgment of the Dutch Supreme Court*. J. Eur. Environ. Plann. Law 17(3), pp. 307–321.

Bass, S. (2020). *The Outdated Third-Party Doctrine and the Need for Modernization*, 65 N.Y.L. SCH. L. REV. 259. pp.259-274.

Bodle, R and Sina, S. (2021). *The German Federal Constitutional Court's decision on the Climate Change Act- Policy Brief. Order of 24 March 2021 - 1 BvR 2656/18 and others.* Ecologic Institute.

Brutti, N. (2005). *Il diritto all'informazione ambientale*, *Profili comparatistici*. Torino, Giappichelli.

Brutti, N. (2022). *Le regole dell'informazione ambientale, tra pubblico e privato.* Estratto. Il diritto dell'informazione e dell'informatica. Anno XXXVIII Fasc. 3. Giuffrè.

Burianski M., Parise Kuhnle F. (2021). *Reshaping Climate Change Law: The German Federal Constitutional Court Orders the German Legislator to Set Clear CO2 Emission Reduction Goals Beyond 2030*. Available at: https://www.whitecase.com/publications/alert/reshaping-climate-change-law

Cavoukian Ann., Polonetsky Jules., Winn Caroline and Information and Privacy Commissioner/Ontario. (2013). *Privacy by Design and Third Party Access to Customer Energy Usage Data*. Toronto Ont: Information and Privacy Commissioner of Ontario Canada. Available at: https://www.deslibris.ca/ID/238739**.**

Chaffey, D. C. (1993). *The Right to Privacy in Canada*. Political Science Quarterly, *108*(1), 117–132. Available at: https://doi.org/10.2307/2152488

Commission of the European Communities. Brussels, 18.7.2001 COM (2001). *Final Green Paper Promoting a European framework for Corporate Social Responsibility.* Available at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2001:0366:FIN:EN:PDF%20

Conseil d' État. (2021). *Greenhouse gas emissions: the Conseil d'État annuls the Government's refusal to take additional measures and orders it to take these measures before 31 March 2022.* Available at: https://www.conseil-etat.fr/en/news/greenhouse-gas-emissions-the-conseil-d-etat-annuls-the-government-s-refusal-to-take-additional-measures-and-orders-it-to-take-these-measures-befor

Cordonier Segger, M-C, Rana, R. et al, (2008). *Selecting Best Policies and Law for Future Generations: legal working paper and worked examples.* World Future Council CISDL. Montreal, Canada.

Court of Justice of the European Union. Luxembourg, 6 October 2020. Press Release No 123/20. Judgments in Case C-623/17, Privacy International, and in Joined Cases C-511/18, La Quadrature du Net and Others, C-512/18, French Data Network and Others, and C-520/18, Ordre des barreaux francophones et germanophone and Others. Press and Information.

Dancey, B C. (2011). *Privacy Implications of Smart Meters.* 86 Chi-Kent L Rev 161 at 182.

Durning, A T. (1992). *How Much is Enough?*. London: Earthscan. pg.29.

Eckes, C. (2022). *Tackling the Climate Crisis with Counter-majoritarian Instruments: Judges Between Political Paralysis, Science, and International Law.* European Papers Vol. 6, 2021, No 3, pp. 1307-1324. Available at: 10.15166/2499-8249/525.

Esty, D C. (2003). *Environmental Protection in the Information Age*. Available at: https://ssrn.com/abstract=429580 or http://dx.doi.org/10.2139/ssrn.429580

European Commission. *Aarhus Convention*. Available at: https://ec.europa.eu/environment/aarhus/

Facts that matter. CBS (2022) *Urgenda reduction target for GHG emissions achieved in 2020.* Available at: https://www.cbs.nl/en-gb/news/2022/06/urgenda-reduction-target-for-ghg-emissions-achieved-in-2020

Ferguson, A. G. (2016). *The Internet of Things and the Fourth Amendment of Effects*. California Law Review, 104(4), 805–880. Available at: http://www.jstor.org/stable/24758739

Fischer Kuh, K. (2012). *Personal Environmental Information: The Promise and Perils of the Emerging Capacity to Identify Individual Environmental Harms*, 65 VAND. L. REV. 1565, 1575–95.

Flachsland, C and Levi, S. (2021). *Germany's Federal Climate Change Act.* Environmental Politics, 30:sup1, 118-140. Available at: 10.1080/09644016.2021.1980288

Ford, D J. et al, (2016). *Big Data has Big Potential for Applications to Climate Change Adaptation* 113:39 NNAS 10729.

Fowler, M. (2018). *Linking the Public Benefit to the Corporation: Blockchain as a Solution for Certification in an Age of Do-Good Business*, 20 Vanderbilt Journal of Entertainment and Technology Law.

Government of Ireland. (2019). *Climate Action Plan to Tackle Climate Breakdown*. Available at: https://webcache.googleusercontent.com/search?q=cache:qh1Qoa1JCToJ:https://assets.gov.ie/10206/d042e174c1654c6ca14f39242fb07d22.pdf&cd=3&hl=it&ct=clnk&gl=it

Government of the Netherlands. *Climate Policy*.
Available at: https://www.government.nl/topics/climate-change/climate-policy

Hirsch, D. (2006). *Protecting the Inner Environment: What Privacy Regulation Can Learn from Environmental Law*. Georgia Law Review, Vol. 41, No. 1, Available at: https://ssrn.com/abstract=1021623

Irizar-Arrieta A., Diego Casado-Mansilla D., Garaizarb P., López-de-Ipiñaa D., Retegib A. (2020). *User perspectives in the design of interactive everyday objects for sustainable behaviour*. International Journal of Human-Computer Studies. Volume 137.

J Harvey, S. (2014). *Smart Meters, Smarter Regulation: Balancing Privacy and Innovation in the Electric Grid.* 61 UCLA L Rev 2068 at 2070.

J. Solove, D. (2006). *A Brief History of Information Privacy Law* in PROSKAUER ON PRIVACY, PLI.

Jawurek, M., Góra J. *Privacy in smart grids*. Engineering dissertation. University of Erlangen–Nuremberg.

Kalkbrenner, A. (2018). *Climate Change, Big Data Revolution and Data Privacy Rights.* 32 J Envtl L & Pract 1 at 6 (WL).

King, K., P.E., CEO, SPEER, Bevill, R., Policy Manager. (2016). *Improving access to smart meter data in Texas.* Speer. The South-central Partnership for Energy Efficiency as a Resource.

Lee, D and J. Hess, D. (2021). *Data privacy and residential smart meters: Comparative analysis and harmonization potential.* Utilities Policy Volume 70**.** Contents lists available at ScienceDirect Utilities Policy.

Litan, R. E. (2001). *Law and Policy in the Age of the Internet*, 50 DUKE L.J. pg. 1045.

Martinez, J., Ruiz, A., Puelles, J., Arechalde, I., Miadzvetskaya, Y. (2020). *Smart Grid Challenges Through the Lens of the European General Data Protection Regulation*. In: Siarheyeva, A., Barry, C., Lang, M., Linger, H., Schneider, C. (eds) Advances in Information Systems Development. ISD 2019. Lecture Notes in Information Systems and Organisation, vol 39. Springer, Cham.
Available at: https://link.springer.com/chapter/10.1007/978-3-030-49644-9_7

Mishra, S. (2022). *The Rise of Climate Litigation.* Harvard Law School Forum on Corporate Governance. Institutional Shareholder Services, Inc.: po.

Orefice, M. (2017). *I big data e gli effetti sulla trasparenza, privacy e iniziativa economica* [tesi di dottorato]. Università degli Studi di Napoli Federico II.

Quinn, E L. (2010). *Smart Metering & Privacy: Existing Law and Competing Policies*.
Report for the Colorado Public Utilities Commission (2009) at 3; Harvey, supra note 13 at
2077 and 2078; US Dept. of Energy, supra note 17 at 26203 and 26205.

Rimmer, M. (2018). *Intellectual property and clean energy: the Paris Agreement and climate justice.* Singapore Springer Singapore.

Rubin, E S. (2010). *Innovation and Climate Change.* Source: NRC. Carnegie Mellon University.

Rubinstein, I. S. (2013). *Big Data: The End of Privacy or a New Beginning?* International Data Privacy Law, Volume 3, No 2.

Sabin Center for Climate Change Law. (2015). U.S. Litigation Chart made in collaboration with Arnold & Porter Kaye Scholer LLP**.** *Urgenda Foundation v. State of the Netherlands.* Available at: http://climatecasechart.com/non-us-case/urgenda-foundation-v-kingdom-of-the-netherlands/

Sabin Center for Climate Change Law. (2017). U.S. Litigation Chart made in collaboration with Arnold & Porter Kaye Scholer LLP**.** *Friends of the Irish Environment v. Ireland.*
Available at: http://climatecasechart.com/non-us-case/friends-of-the-irish-environment-v-ireland/

Sabin Center for Climate Change Law. (2020) U.S. Litigation Chart made in collaboration with Arnold & Porter Kaye Scholer LLP. *Neubauer, et al. v. Germany.*
Available at: http://climatecasechart.com/non-us-case/neubauer-et-al-v-germany /

Sebestyén, V, Czvetkó, T and Abonyi, J. (2021). *The Applicability of Big Data in Climate Change Research: The Importance of System of Systems Thinking.* Front. Environ. Sci. 9:619092. Available at: 10.3389/fenvs.2021.619092.

Shannon, N. de Wit, E. (2019). *Urgenda Foundation v Netherlands: Historic climate change decision upheld***.**
Available at: https://www.nortonrosefulbright.com/en-au/knowledge/publications/45dc4f83/urgenda-foundation-v-netherlands-historic-climate-change-decision-upheld

Sweeney, L. (2002). *k-Anonymity: A model for protecting privacy*. International Journal on Uncertainty, Fuzziness and Knowledge-Based Systems. 10:557{570.

The European Union Agency for Cybersecurity (ENISA). (2015). *Privacy by design in big data: An overview of privacy enhancing technologies in the era of big data an alytic.* PO Box 1309, 710 01 Heraklion, Greece. Available at:10.2824/6410

U.S. Department of Energy. (2011). City of Naperville Case Study. *At the Forefront of the Smart Grid: Empowering Consumers in Naperville, Illinois.* Final Submitted to NREL.

Thompson, R M. II. (2014). *The Fourth Amendment Third-Party Doctrine*. Report. Washington D.C. University of North Texas Libraries, UNT Digital Library.

U.S. Department of Health, Education, and Welfare. (1973). *Records, Computers, and the Rights of Citizens*: Report of the Secretary's Advisory Comm. On Automated Personal Data Systems. Available at: https://www.justice.gov/opcl/docs/rec-com-rights.pdf

Vergason, D. (2021). *Preventing the impending death of privacy by the Smart Grid.* Lewis & Clark Law School. Environmental Law, 2021, Vol. 51, No. 2 pp. 549-575.

Vos J. (2009). *Actions speak louder than words: greenwashing in corporate America*. Notre Dame JL Ethics Pub Policy 23:673.

Wang, X, Dang, Q, Guo, J and Ge, H. (2013). *RFID Application of Smart Grid for Asset Management.* International Journal of Antennas and Propagation. Vol. 2013, no. 2013, pp.1-6.

Whittaker, M. (2022). *Public Benefit Corporation vs. B Corp: What's the Difference?* Available at: https://money.usnews.com/investing/articles/public-benefit-corporation-vs-b-corp-whats-the-difference

Zeadally, S, Pathan, A, Alcaraz, C, and Badra, M. (2013). *Towards Privacy Protection in Smart Grid.* Article *in* Wireless Personal Communications. Available at: 10.1007/s11277-012-0939-1.

Online References

Algorand. *PlanetWatch Environmental***.** https://www.algorand.com/ecosystem/use-cases/planetwatch

At internet. CLIL. https://www.atinternet.com/en/glossary/cnil/

buildd. *PBC Company - Definition of Public Benefit Corporation & Compare PBC vs B Corp vs Nonprofits.* https://buildd.co/funding/public-benefit-corporation

California. Public Utilities Commission. *Energy Data Access Committee (EDAC).* https://www.cpuc.ca.gov/industries-and-topics/electrical-energy/demand-side-management/energy-efficiency/energy-data-access-committee

Casetext. *State v. Kluss.* https://casetext.com/case/state-v-kluss

Cranium. *Smart Energy and GDPR for utility.* https://gdpr.be/uncategorized/smart-energy-gdpr-utility/

Cern Accelerating science. *CERN air-quality data analysis spin-off raises 1.2 million euros in funding.* https://kt.cern/content/cern-air-quality-data-analysis-spin-raises-12-million-euros-funding

Commission of the European Communities, 2001b, p. 6. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52006DC0136:EN:HTML

Conseil d'État. (2021). *Greenhouse gas emissions: the Conseil d'État annuls the Government's refusal to take additional measures and orders it to take these measures before 31 March 2022.* https://www.conseil-etat.fr/en/news/greenhouse-gas-emissions-the-conseil-d-etat-annuls-the-government-s-refusal-to-take-additional-measures-and-orders-it-to-take-these-measures-befor

Cornell Law School. Legal Information Institute. https://www.law.cornell.edu/wex/fourth_amendment#:~:text=A%20search%20or%20seizure%20is,search%20or%20seizure%20is%20justified

Court Listener. https://www.courtlistener.com/opinion/107564/katz-v-united-states/summaries/**?**

Crunchbase. GoodGuide. https://www.crunchbase.com/organization/goodguide

Crunchbase. Provenance. https://www.crunchbase.com/organization/provenance

Data for Climate Action. https://www.unglobalpulse.org/challenges-hackathons/data-for-climate-action/

Electric Energy Online. Green Ovations: Innovations in Green Technologies. *More Power, Less Energy: Power to the People.* https://electricenergyonline.com/energy/magazine/618/article/Green-Ovations-Innovations-in-Green-Technologies.htm

Electronic Paper (2020). *Application and importance of RFID technology in Smart Grid.* https://ee-paper.com/application-and-importance-of-rfid-technology-in-smart-grid/

Elevate Energy. Smarter energy use for all. *Aggregated Data Access: The 15/15 Rule in Illinois and Beyond.* https://elevatenp.org/wp-content/uploads/1515-Rule-Factsheet-FINAL.pdf

European Commission. Aarhus Convention. https://ec.europa.eu/environment/aarhus/

Facts that matter. CBS (2022) *Urgenda reduction target for GHG emissions achieved in 2020*. https://www.cbs.nl/en-gb/news/2022/06/urgenda-reduction-target-for-ghg-emissions-achieved-in-2020

Government Technology. (2010). *Hoboken, N.J., Battles Parking Permit Counterfeiting With RFID System.* https://www.govtech.com/public-safety/hoboken-nj-battles-parking-permit-counterfeiting.html

Iberdrola. *DSO — how to convert grid management towards a smarter system?* https://www.iberdrola.com/innovation/distribution-system-operation

Iea (2017) *Energy Efficiency Benchmarking Covenant.* https://www.iea.org/policies/1605-energy-efficiency-benchmarking-covenant

Independent transport research organisation with a mission to accelerate and support the switch to electric vehicles in the UK. https://newautomotive.org/

International Monetary Fund. *Externalities: Prices Do Not Capture All Costs.*

https://www.imf.org/external/pubs/ft/fandd/basics/external.htm

Intersoft consulting. Art. 35 GDPR- *Data protection impact assessment.* https://gdpr-info.eu/art-35-gdpr/

Investopedia. *Tragedy of the Commons: What It Means in Economics* https://www.investopedia.com/terms/t/tragedy-of-the-commons.asp

Jdsupra. *German Constitutional Court rejects complaints against federal states' climate protection laws.* https://www.jdsupra.com/legalnews/german-constitutional-court-rejects-8338418/

Justia US Law. *Naperville Smart Meter Awareness v. City of Naperville, No. 16-3766 (7th Cir. 2018)* https://law.justia.com/cases/federal/appellate-courts/ca7/16-3766/16-3766-2018-08-16.html

Justia. US Supreme Court. Kyllo v. United States, 533 U.S. 27 (2001) https://supreme.justia.com/cases/federal/us/533/27/

Khan Academy. *Command-and-control regulation.* https://www.khanacademy.org/economics-finance-domain/microeconomics/market-failure-and-the-role-of-government/environmental-regulation/a/command-and-control-regulation-cnx

Lawfare. *Third-Party Party-Crashing? The Fate of the Third-Party Doctrine* https://www.lawfareblog.com/third-party-party-crashing-fate-third-party-doctrine

Legal Information Institute: Open access to law since 1992. *42 U.S. Code § 4331 - Congressional declaration of national environmental policy.* https://www.law.cornell.edu/uscode/text/42/4331#:~:text=The%20Congress%20recognizes%20that%20each,I%2C%20%C2%A7%20101%2C%20Jan.

LexisNexis. *Silverman v. United States - 365 U.S. 505, 81 S. Ct. 679 (1961).* https://www.lexisnexis.com/community/casebrief/p/casebrief-silverman-v-united-states

Luiss Open. (2021). *Perché la storica sentenza tedesca impone una riflessione sulla responsabilità intergenerazionale.* https://open.luiss.it/2021/05/28/perche-la-storica-sentenza-tedesca-impone-una-riflessione-sulla-responsabilita-intergenerazionale/

Lowtry Solutions. *What is the Future of RFID Technology?* https://lowrysolutions.com/blog/what-is-the-future-of-rfid-technology/

National Constitution Center. Supreme Court Case. Katz v. United States. 389 U.S. 347 (1967). https://constitutioncenter.org/the-constitution/supreme-court-case-library/katz-v-united-states#:~:text=.%20.%20.%20.-,%5BT%5Dhe%20Fourth%20Amendment%20protects%20people%

NCSL. Shea, D. and Bell, K. (2019). *Smart Meter Opt-Out Policies.* https://www.ncsl.org/research/energy/smart-meter-opt-out-policies.aspx

OECD. *Introduction to Pollutant Release and Transfer Registers (PRTRs).* https://www.oecd.org/env/ehs/pollutant-release-transfer-register/introductionto-pollutant-release-and-transfer-registers.htm

Ohm, P. (2012). Harvard Business Review. *Don't Build a Database of Ruin.* https://hbr.org/2012/08/dont-build-a-database-of-ruin

OLR Research Report. (1999). *Searches by administrative agencies.* https://www.cga.ct.gov/PS99/rpt%5Colr%5Chtm/99-R-0265.htm

Oracle Netsuit. Abby Jenkins. *What Is Demand Management: Functions, Process and Examples.* https://www.netsuite.com/portal/resource/articles/inventory-management/demand-management.shtml

Planet Watch White Paper. https://www.planetwatch.io/white-paper/html5forwebkit.html

Plumer, B. (2015). *Volkswagen's appalling clean diesel scandal, explained.* https://www.vox.com/2015/9/21/9365667/volkswagen-clean-diesel-recall-passenger-cars

Protecting Privacy. Promoting Trust in Government. *Fair Information Practice Principles (FIPPs).* https://www.fpc.gov/resources/fipps/

Science Direct. *Privacy Impact Assessment.* https://www.sciencedirect.com/topics/computer-science/privacy-impact-assessment

Shannon, N. de Wit, E. (2019) *Urgenda Foundation v Netherlands: Historic climate change decision upheld.* https://www.nortonrosefulbright.com/en-au/knowledge/publications/45dc4f83/urgenda-foundation-v-netherlands-historic-climate-change-decision-upheld

Sheppard, White, Kachergus, DeMaggio P.A. *Search and Seizure: Expectation of Privacy and the Physical Intrusion Test.* https://www.sheppardwhite.com/blog/2013/07/search-and-seizure-expectation-of-privacy-and-the-physical-intrusion-test/

State of California Department of Justice. *California Consumer Privacy Act (CCPA).* https://oag.ca.gov/privacy/ccpa

Techopedia. *Safe Harbor- What Does Safe Harbor Mean?* https://www.techopedia.com/definition/14227/safe-harbor

TechTarget. *Fair Information Practices (FIP).* https://www.techtarget.com/whatis/definition/Fair-Information-Practices-FIP#:~:text=FIP%20(Fair%20Information%20Practices)%20is,issues%20of%20privacy%20and%20accuracy

TechTarget Network (2022). *What is the internet of things (IoT)?* https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT

The Guardian. (2021). *How data could save Earth from climate change.* https://www.theguardian.com/environment/2021/jul/18/how-data-could-save-earth-from-climate-change

The Paris Rulebook After COP26. https://www.allenovery.com/en-gb/global/blogs/countdown-to-cop/the-paris-rulebook-after-cop26

Ubisecure. (2022). *Privacy by Design, with Ann Cavoukian, Global Privacy and Security by Design Centre.* https://www.ubisecure.com/podcast/privacy-by-design-ann-cavoukian/

U.S. Department of Health, Education, and Welfare. (1973). *Records, Computers, and the Rights of Citizens*: Report of the Secretary's Advisory Comm. On Automated Personal Data Systems. https://www.justice.gov/opcl/docs/rec-com-rights.pdf

US Legal. *Lex Specialis Law and Legal Definition.* https://definitions.uslegal.com/l/lex-specialis/

W. Jeffrey Howard, Phillip Townsend Associates. *Execution Experience with the Dutch Energy Efficiency Benchmarking Covenant between the Government and the Chemical Industry.* pg.155. https://webcache.googleusercontent.com/search?q=cache:LPx2SFlFlnYJ:https://aceee.org/files/proceedings/2001/data/papers/SS01_Panel2_Paper15.pdf&cd=7&hl=it&ct=clnk&gl=it

Wagner, A., Speiser, S., Harth, A., Raabe, O., Weis, E. Karlsruhe Institute of Technology. *Basic Privacy Principles for the Smart Grid.* https://www.w3.org/2010/api-privacy-ws/papers/privacy-ws-20/

World Health Organization. *Air pollution*. https://www.who.int/health-topics/air-pollution#tab=tab_1

Yale journal on regulation/Bernard Bell**.** (2018). *Too Smart by Half?: Naperville Smart Meter Awareness v. City of Naperville.* https://www.yalejreg.com/nc/too-smart-by-half-naperville-smart-meter-awareness-v-city-of-naperville/