Journal of Law, Technology & Trust
Vol. 2 No. 1 (2021): JLTT Volume 2 Issue 1 (Advance Access Articles)

Smart meters' roll out, solutions in favour of a trust enhancing law in the EU

Domenico Orlando; Wim Vandevelde*

1. Introduction

The roll-out of smart meters in the EU and the resulting digitalization of the electricity grid present both opportunities and potential risks to society. On the one hand it offers, among other things, efficient management, distribution and consumption of energy, as well as a more feasible and efficient transition towards renewable energy sources. On the other hand, it involves the collection and processing of large amounts of personal data, from which concerns and risks emerge in the field of privacy and data protection. The widespread processing of these personal data for varying purposes can be seen as invasive by revealing details on people's lifestyles and daily habits.

Genuine concerns and risks related to the collection and processing of personal data by smart meters result in ascertain ambivalence towards, and consequently a lack of trust in, the technology. The question then arises whether, taking into account the identified concerns and risks, the existing privacy, data protection, and energy frameworks offer sufficient guarantees for the protection of the rights and freedoms of citizens, thereby enhancing trust in the technology. We approach this question by first identifying the gaps in the existing EU legislative framework that are detrimental to the trust in, and consequently the acceptance of, smart meters. This exercise is followed by an analysis of the relevant legislation in Flanders, Belgium, to see whether these gaps can be effectively remedied on the national level. Finally, based on the lessons learned, we propose appropriate solutions to address the shortcomings of the EU legislative frameworks, thereby mitigating some of the identified concerns and risks in order to enhance trust in smart meters.

2. Overview of the technology

The 'smart meter' is an appliance that measures the consumption and production of electricity with enhanced granularity (every hour, quarter of an hour or even every minute) and which is able to store and communicate this information through digital technologies. What makes a meter of the new generation different from a traditional meter: (i) the collection of more detailed data and their conversion in a digital form, (ii) the communication of such data through a digital infrastructure that allows bits to travel in parallel to electricity,[1] (iii) the control that companies can exercise remotely over the appliance, with the possibility, for instance, to shut down the provision of electricity. So the consumption and production will not be checked every year or so by a clerk ringing

* The authors both research in law at the Center for IT and IP law, KU Leuven. A special thank goes to Professor Anton Vedder for his precious advise and support. The research has been conducted in the scope of the projects of SNIPPET and ROLECS, financed by the Government of Flanders.

[1] The bits may be transmitted directly on the electricity cable, through a technology called power line communication (PLC) or via wireless. In the case of wireless the expression "bits that travel in parallel to electricity" is intended merely as a metaphor.

the doorbell of users, a scene that belongs to the old world, but rather be transmitted via wires or even wireless to the operators. A smart meter can function in the sectors of water and gas measurement as well, but these applications will be disregarded in the present article.

The whole grid is now called 'smart' and the smart meter is just the endpoint of the broader electricity grid. This 'smart grid' consists of smart meters, sensors and advanced computer systems all spread throughout the low, medium and high voltage lines of distribution, transmission and control.

The smart meters have several advantages for the efficient management of electricity production, distribution and consumption. In fact, by knowing the exact and real-time amount of electricity consumed and produced, companies operating on the grid can fulfil their task of keeping the offer and demand in good balance, the grid in tension and the electricity constantly available for homes, offices, factories and public buildings.

It would make perfect sense to call the described phenomenon 'electricity digitalisation', a term tying together two technologies. One, electricity, already in existence, pervasive and allowing for the second industrial revolution; and the other, digitalisation, which makes computation and communication smooth and immediate at long distances.

3. Opportunities

The digitalisation of the grid is the source of different opportunities in the electricity field. Firstly, it makes the plans for a greener world more sound and feasible. Indeed the renewable sources of electricity have an inherent limit, namely that they depend on atmospheric variables. The solar energy depends on the solar radiation and the wind energy depends on a constant wind. There do not yet exist huge batteries that allow for the storage of large quantities of electricity to release on the grid whenever a cloudy day or a day without wind occurs, while the grid needs a continuous stimulus per se. The entire system can rely more on renewable sources only if it is possible to monitor multiple factors in real-time, by crossing accurate weather forecasts with detailed consumption previsions based on workloads' trends. Otherwise, renewable and non-polluting sources will be relegated to the role of gregarious compared to the traditional coal, nuclear or oil run plants, contrary to the objects of the Green New Deal and its latter relaunch by the EU Commission.[2]

Secondly, the monitoring made possible by the digitalisation is an enabler for a new asset of the grid too, where the production is not concentrated only in the central plants. Now, and even more so in the future, electricity production is not just centralised but rather involves small producers with photovoltaic panels on the roof and wind turbines in the garden.[3] Monitoring a big plant is easier than performing the same task in many small

[2] European Commission, *The European Green Deal*, December 11 2019, https://ec.europa.eu/info/sites/info/files/european-green-deal-communication_en.pdf; https://ec.europa.eu/clima/policies/eu-climate-action/2030_ctp_en .

[3] Just in Italy, production centers have passed from 800 to 800.000 in ten years. Celestina Dominelli, "Nuovo piano terna a novembre per accompagnare il cambiamento", *Il Sole 24 Ore*, September 29, 2020. Video, 15:58. https://stream24.ilsole24ore.com/video/economia/nuovo-piano-terna-novembre-accompagnare-cambiamento/ADsYPUs.

production units. Digital technology could also help in this sense. The fact that the production is decentralised has consequences in the electricity market as well. The consumer is not just a passive figure anymore but is also a producer; from the merge of these two terms we get the hybrid 'prosumer'. The prosumer consumes, produces and, why not, trades electricity with the utilities and other prosumers. New prototypes of peer-to-peer markets are emerging where electricity is traded via online platforms.

Finally, the use of electricity expands to new sectors like mobility and heating. For environmental reasons, new cars will be powered by electricity and the same applies to, for example, electric boilers. Indeed, vehicles and heating systems run by electricity have less impact on air quality.

4. Privacy and data protection risks

Smart meters collect granular data about electricity consumption,[4] from which it is possible to infer customers' behavioural patterns in detail. The technology is so precise that it allows a trained eye (not necessarily a human one) to identify which appliances are turned on in a home based on the watt consumed (see Figure 1). [5]

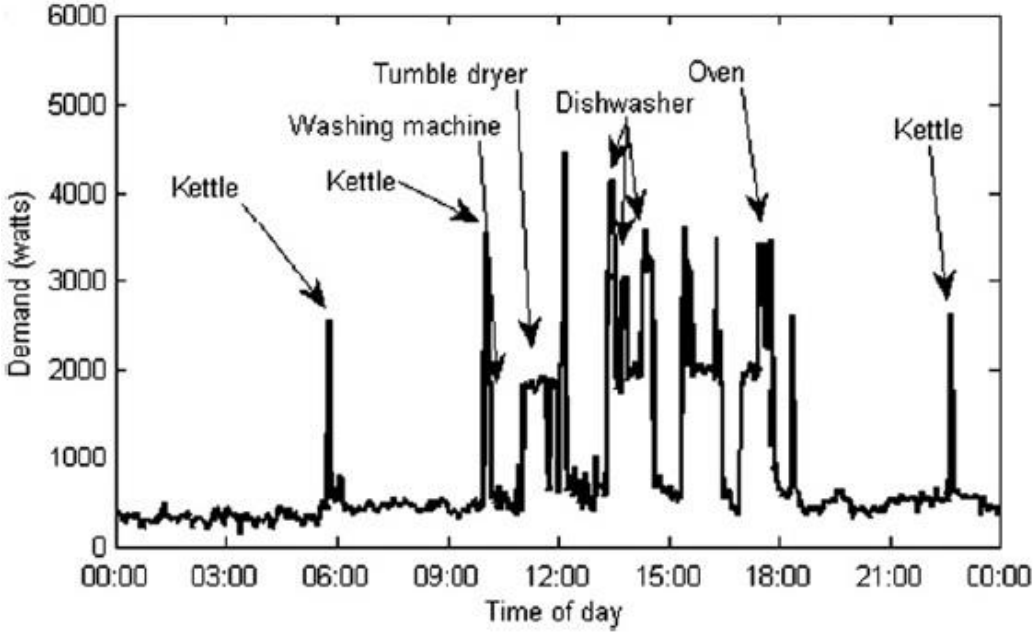

Figure 1: *Demand data for single dwelling collected over 1 minute interval*. Source: McKenna, Smart meter data: Balancing consumer privacy concerns with legitimate application, 2011.

[4] Granular data is detailed data, or the lowest level that data can be in a target set. "Granular Data," Techopedia, accessed December 16, 2019, https://www.techopedia.com/definition/31722/granular-data).
[5] Megane Mclean, "How Smart Is Too Smart? How Privacy Concerns Threaten Modern Energy Infrastructure," *Vanderbilt Journal of Entertainment and Technology* Law 18, no. 4 (Summer 2016), 885.

The specific uses of such detailed data are manifold and disparate. For instance, electricity data could reveal whether a security alarm system is present as well as if it is turned on or off.[6] The time of charging and the battery level of an electric vehicle might disclose one's travel habits.[7] Cleaning habits and personal hygiene routines might likewise be inferred by the use of the shower, washing machine, etc.[8] Through electricity data it is possible to know if particular medical equipment is in use in a home, and how it is used.[9] Some researchers affirm to be able to discover not just if a TV is active or not, but even which channel is being watched at any moment.[10] Electricity data can reveal how many people inhabit a house,[11] and whether they are inside the house at a precise moment.[12]

Apart from the directly involved utility services, several other entities could be interested in collecting and processing such data. Insurance companies might be interested in their clients' lifestyle and health conditions,[13] the marketing industry could use profiling to target potential clients with products,[14] and last but not least, the government, police and judiciary. Tax authorities might be interested in confirming the main place of residence

---

[6] Ibid.

[7] Balough, Cheryl D. "Privacy Implications of Smart Meters", *Chicago Kent Law Review* 86, no 1 (2011), 168; Forbush, John R. "Regulating the Use and Sharing of Energy Consumption Data: Assessing California's SB 1476 Smart Meter Privacy Statute," *Albany Law Review* 79, no. 1 (Fall 2011), 349; Jonida Milaj and Jeanne Pia Misfud Bonnici, "Privacy Issues in the Use of Smart Meters- Law Enforcement Use of Smart Meter Data", in *Smart Grids from a Global Perspective* ed. Beaulier, de Wilde and Scherper (Springer International Publishing Switzerland), 180; Harvey, Samuel J. "Smart Meters, Smarter Regulation: Balancing Privacy and Innovation in the Electric Grid," *UCLA Law Review* 61, no. 6 (July 2014), 2078; Fan, Zhong, Kalogridis, Georgios et al., "The New Frontier of Communications Research: Smart Grid and Smart Metering," *E-Energy*, proceedings of 1st International Conference on Energy-Efficient Computing and Networking (2010): 117; Cavoukian, Ann, Polonetsky, Jules "SmartPrivacy for the Smart Grid: Embedding Privacy into the Design of Electricity Conservation," *Identity in the Information Society* 3, no. 2 (2010): 284.

[8]Forbush, "Regulating the use and Sharing of Energy Consumption data", 349; Zeadally, Sherali and Pathan, Al-Sakib, "Towards Privacy Protection in Smart Grid," *Wireless Personal Communications* 73, no. 1 (2013): 32; European Data Protection Supervisor, *Opinion on the Commission Recommendation on preparations for the roll-out of smart metering system*, (2012), 4; Cavoukian and Polonetsky, "SmartPrivacy for the Smart Grid", 284.

[9] Harvey, "Smart Meters, Smarter Regulation", 2078; Mclean, "How Smart is Too Smart", 885; EDPS, Opinion for the roll-out of smart metering system, 4.

[10] Harvey, "Smart Meters, Smarter Regulation", 2078; Zhu, Liehuang, Zhang, Zijian and Xu, Chang, "Privacy-preserving Meter Reading Transmission in Smart Grid," in *Secure and Privacy-preserving Data Communication in Internet of Things* (SpringerBriefs in Electrical and Computer Engineering, 2017), 35; Zeadally Pathan, "Towards Privacy Protection in Smart Grid", 32; Cavoukian and Polonetsky, "SmartPrivacy for the Smart Grid", 284; EDPS, Opinion for the roll-out of smart metering system, 5.

[11] Zeadally Pathan, "Towards Privacy Protection in Smart Grid", 32.

[12] Zeadally Pathan, "Towards Privacy Protection in Smart Grid", 32; Cavoukian and Polonetsky, "SmartPrivacy for the Smart Grid", 284.

[13] Forbush, "Regulating the use and Sharing of Energy Consumption data", 349; Milaj Bonnici, "Privacy issues in the Use of Smart Meters", 180; EDPS, Opinion for the roll-out of smart metering system, 6.

[14] Forbush, "Regulating the use and Sharing of Energy Consumption data", 349; Milaj Bonnici, "Privacy issues in the Use of Smart Meters", 180; Nancy J. King and Pernille W. Jessen, "For Privacy's Sake: Consumer 'opt outs' for Smart Meters*," Computer Law & Security Review: The International Journal of Technology Law and Practice* 30, no. 5 (October 2014), 532; Savirimuthu, "Smart Meters and the Information Panopticon: beyond the Rethoric of Compliance", 165; Cavoukian and Polonetsky, "SmartPrivacy for the Smart Grid", 284; EDPS, Opinion for the roll-out of smart metering system; Balough, "Privacy Implications of Smart Meters", 188.

indicated by a taxpayer, while law enforcement could use electricity data in investigations.[15] For example, this was the case when the abnormal consumption of electricity in some apartments helped the authorities discover marijuana plantations, given that these activities required a prolonged usage of lamps.[16] In addition to these situations, in the wake of coronavirus, we could add the sanitary authority that checks if a positive subject is observing the quarantine or the employer verifying if the employee is actually at home during the smart working.

Malevolent actors could find electricity data useful as well. This is the case for burglars or stalkers interested in knowing if a house has a security alarm and whether or not it is occupied.[17]

Moreover, the roll-out of invasive smart meters is envisaged by the EU in the scope of a political program with an impact on households, and the latter might not be able to refuse their installation.[18] We will come back on this point later on.

5. Where does trust come in?

Smart meters are not just another piece of the broader puzzle of the mass surveillance phenomenon, but an especially critical point, since electricity data are often linked to one's home, where there are heightened expectations of privacy, safety and freedom to be oneself.[19] The home is rightly perceived as an inviolable bastion. In *Dogville*, a 2003 movie by the Danish director Lars Von Trier, the homes are exposed, because the walls are represented by just chalk lines on the floor (see Figure 2). Thus, in the cinematographic experiment, the spectator is able to see both the individuals on the streets and the ones inside their homes. The film shows blatantly that the attitude and postures of the persons inside their homes are much different from the ones outdoors. What happens inside is not meant to be observed from the outside, and this is one of the reasons behind the invention of very basic and successful technologies such as curtains.

Hostile sentiments towards the smart meters have materialised both in the USA, the Netherlands and Germany. In 2009, the Dutch Senate, following consumer association pressures, rejected a Smart Metering Bill, which would have mandated the installation of smart meters in every home. The first proposal was followed by a text which was much more supportive of the data protection cause, allowing customers to oppose installation.[20]

---

[15] Forbush, "Regulating the use and Sharing of Energy Consumption data", 349; Knyrim, Rainer and Trieb, Gerald "Smart Metering under EU Data Protection Law," *International Data Privacy Law* 1, no. 2 (2011): 122; Savirimuthu, "Smart Meters and the Information Panopticon: beyond the Rethoric of Compliance", 165; Mclean, "How Smart is too Smart?", 885; EDPS, Opinion for the roll-out of smart metering system, 6.
[16] Glenn Smith, " Marijuana bust shines light on utilities," *The Post and Courier*, January 28, 2012 updated November 2, 2016, https://www.postandcourier.com/news/marijuana-bust-shines-light-on-utilities/article_f63a8bed-9a43-5429-aaef-99f7eb0f71f0.html.
[17] Forbush, "Regulating the use and Sharing of Energy Consumption data", 349; Balough, "Privacy Implications of Smart Meters", 168.
[18] King and Jessen, "For Privacy's Sake: Consumer 'opt outs' for Smart Meters", 535.
[19] George William Hart, "Residential Energy Monitoring and Computerized Surveillance via Utility Power Flows", *IEEE Technology and Society Magazine*, (June/July 1989): 12.
[20] Rainer Knyrim and Gerald Trieb, "Smart Metering under EU Data Protection Law", *International Data Privacy Law 1*, no. 2 (2011), 122; Eoghan Mckenna, Ian Richardson, and Murray Thomson, "Smart Meter Data: Balancing Consumer Privacy Concerns with Legitimate Applications", *Energy Policy 41* (February

In Germany, a civil rights and privacy campaign group awarded an electricity supplier, which had planned to install smart meters, with the infamous 'Big Brother' prize.[21] In California (U.S), in the city of Ojai, the local council approved a total ban on smart meters because, amongst other reasons, they were "*subjecting residents of Ojai to privacy* (…) *risks*".[22] Other communities in California and the U.S have taken resolutions in the same direction and have shown their intolerance vis-a-vis smart meters.[23]

Figure 2: The set of *Dogville* (2003)

Scepticism towards smart meters has spread on the internet as well, for instance by blogs dedicated to smart grid and smart meters that bring up privacy and health consequences of the technology.[24] One thing is clear: smart meters currently suffer from a lack of trust. This is understandable given the accompanying risks.

2012), 807; Abbe Brown and Rónán Kennedy, "Regulating Intersectional Activity: Privacy and Energy Efficiency, Laws and Technology", *International Review of Law, Computers & Technology 31*, no. 3 (September 2017), 348.

[21] Mckenna, "Smart Meter Data: Balancing Consumer Privacy concerns with Legitimate Applications", 807; Jonida Milaj and Jeanne Pia Misfud Bonnici, "Privacy Issues in the Use of Smart Meters- Law Enforcement Use of Smart Meter Data", in *Smart Grids from a Global Perspective* (Springer International Publishing Switzerland), 180.

[22] City of Ojai Ordinance No. 823 May 29, 2012, accessed June 26, 2019, http://emfsafetynetwork.org/wp-content/uploads/2009/11/Ojai-Ordinance-823-Smart-Meters.pdf.

[23] Liehuang Zhu, Zijian Zhang, and Chang Xu, "Privacy-preserving Meter Reading Transmission in Smart Grid," in *Secure and Privacy-preserving Data Communication in Internet of Things* (SpringerBriefs in Electrical and Computer Engineering, 2017), 34; Samuel J. Harvey, "Smart Meters, Smarter Regulation: Balancing Privacy and Innovation in the Electric Grid," *UCLA Law Review 61*, no. 6 (July 2014), 2084; Megane Mclean, "How Smart Is Too Smart? How Privacy Concerns Threaten Modern Energy Infrastructure," *Vanderbilt Journal of Entertainment and Technology Law 18*, no. 4 (Summer 2016), 881.

[24] K.T Weaver, Smart Grid Awareness, https://smartgridawareness.org, last accessed October, 19 2020; Stop smart meters! https://stopsmartmeters.org, accessed October, 23 2020; Coalition to stop smart meters, https://stopsmartmetersbc.com, accessed October, 23 2020. In these blogs concern is expressed on the radiation allegedly emitted by the smart meters.

One could be tempted to associate the privacy and data protection concerns around smart meters with the ones affecting the Internet of Things (IoT) technologies because often the IoT technologies are found in the home as well (think of Alexa by Amazon). However, there is an important difference, namely that smart meters are being installed following a political target to be reached: 80% of EU customers to be equipped with smart meters by 2020.[25] While purchasing an IoT technology and putting it in the living room is a deliberate and conscious choice made by the consumers. Smart meters are often installed without the option to refuse them.

In addition to the trust of customers, we think that the trust (or reliance on) of operators should be taken into account as well. We presume that the distribution service operators, who usually own the meters and are responsible for their functioning, require a clear framework that allows them to invest in innovation while avoiding the risk of halting the adoption of smart meters due to the mistrust of customers. It is in their own interest that concerns for privacy and data protection are tackled in advance. It would be ideal for them to have a precise law that establishes obligations without gaps and uncertainties, a law they can comply with in order not to be held liable for damages and avoid sanctions.

6. Where does the law come in?

6.1 Privacy and data protection law

Article 8 of the European Convention on Human Rights (ECHR)[26]by the Council of Europe and Article 7 of the Charter of Fundamental Rights of European Union (CFREU)[27] by the EU both tackle the right to privacy, attributing it with the highest protection in the scale of rights and focussing on the special shield reserved for the 'home', which is explicitly mentioned in the provisions.

It is worth mentioning that the European Court of Human Rights of Strasbourg has included the office under the definition of home in the *Société Colas Est and others* v. *France* case,[28] and by doing so extending the application of the mentioned provision to the "*homes of juristic persons*".

Article 8 CFREU stresses the necessity to protect personal data as well. Privacy and data protection are two intertwined concepts, which have a reciprocal bilateral relation, in the sense that private personal data are included in the common sphere of influence of privacy and data protection. Differently, privacy is exclusively engaged with other aspects of the private life such as personal relations and the body integrity, while data protection deals

[25] Directive 2009/72/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in electricity and repealing Directive 2003/54/EC, OJ L 211, 14.8.2009, p. 55–93, Annex II, section 2, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32009L0072.
[26] European Convention on Human Rights as amended by Protocols Nos. 11 and 14 and supplemented by Protocols Nos. 1, 4, 6, 7, 12, 13 and 16, Council of Europe, Rome, 4 November 1950, https://www.echr.coe.int/Documents/Convention_ENG.pdf.
[27] Charter of Fundamental Rights of European Union, OJC 326, 26.10.2012, p. 391-407, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT.
[28] Société Colas Est and others v. France, European Court of Human Rights, 16 April 2002.

with the processing of personal data in general, whether private or public in nature.[29] This is, however, not the occasion to go into details It suffices to notice that the highest level of legal protection for customers in the use of the smart meters is widely covered.

Going one step down in the hierarchy of norms, the attention for data protection is major. The General Data Protection Regulation (GDPR) remarkably enhances data protection rights and directly imposes obligations in the EU since 2018.[30] It is often considered a model for data protection laws around the world. The GDPR is a technologically neutral law, because it applies to any kind of data processing happening with physical files or digital files, and it is a horizontal law because it applies to any sector, that could be finance, health, electricity and so on. Within the smart grid, the application of the GDPR is triggered by the classification of personal data under Article 4.1. The definition is very broad: "*any information related to an identified or identifiable person*". Thus, in the electricity sector, many data will qualify as personal. From the name to the address, from the bank account number to the meter number and, here we have the novelty, the smart meter's workload, including the electricity consumption and, in an age of prosumers, the electricity production.

The Spanish Supreme Court, applying the EU data protection law, has established that data about the electricity consumption are personal data. The controversy arose about an administrative regulation which obliged the Distribution Service Operator (DSO), responsible for reading the meters, to share the consumption workload of customers with the Transmission Service Operator (TSO), for system management reasons.[31]

6.2 Energy law

It is a settled principle that the *lex specialis* would prevail, in case of contrast, over the *lex generalis*. So Energy Law would prevail over the GDPR when dealing with data protection in this specific sector.[32]The relevant laws that deal with smart meters are the Directive for the Internal Market in Electricity 2019/944/EU,[33] and the Energy Efficiency Directive 2012/27/EU,[34] as subsequently amended in 2013 and 2018.[35]

---

[29] Lamanuzzi, Marta, "Diritto penale e trattamento dei dati personali: Codice della privacy, novità introdotte dal regolamento 2016/679/UE", *Jus-online*, n. 1/2017: 223.
[30] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1–88, https://eur-lex.europa.eu/eli/reg/2016/679/oj.
[31] Tribunal Supremo Sala de contencioso, 12/07/2019, Iberdrola Distribucion Electrice v. Red Electrica de Espana.
[32] Alessandra Fratini and Giulia Pizza, "Data Protection and Smart Meters: The GDPR and the 'winter Package' of EU Clean Energy Law," EU Law Analysis, March 22, 2018, accessed July 17, 2019, http://eulawanalysis.blogspot.com/2018/03/data-protection-and-smart-meters-gdpr.html.
[33] Directive 2019/944/EU of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU, OJ L 158, 14.6.2019, p. 125-199.
[34] Directive 2012/27/EU of the European Parliament and of the Council of 25 October 2012 on energy efficiency, OJ L 315, 14.11.2012, p. 1–56.
[35] Council Directive 2013/12/EU, Directive 2018/844/EU, Directive 2018/2002/EU, Regulation 2018/1999/EU, see the consolidated version at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02012L0027-20181224, accessed 19 July 2019.

The Internal Market in Electricity Directive deals with smart meters from Article 19 to 23. Article 19.1 already mentions a relation of 'accordance' between the whole smart metering system and unspecified 'Union data protection rules'. Article 20, devoted to smart metering systems functionalities, focuses on cybersecurity (point b) as well as privacy and data protection (point c). Point (e) of the same article stresses the concept of availability of customer's data for purposes of interoperability and data portability. Point (f) ensures that the customers get all the necessary information about the potentials of monitoring energy consumptions and "*concerning the collection and processing of personal data*", in a similar way as Article 13 GDPR, which sets out the right to information.

Article 23, titled *Data management*, insists on the access to data by any eligible party. However, the concept of 'eligible party' is not further specified in the Directive.

The Energy Efficiency Directive 2012/27/EU,[36] as subsequently amended in 2013 and 2018,[37] addresses the smart meters topic in Article 9, which covers metering in general. Paragraph 1 calls the Member States for the provision of "(…)*individual meters that accurately reflect* (…) *actual energy consumption and that provide information on the actual time of use*". The 'smartness' is not precisely mentioned here, but the paraphrase reflects the same idea. Paragraph 2 directly mentions the smart meters, recalling the Internal Market in Electricity Directive and, under point b), requires security in data communication and privacy of final customers in compliance with relevant Union data protection and privacy legislation. Also point e) is relevant, as it establishes that appropriate advice and information are to be provided to the final customer at the moment of the installation of the smart meters, particularly about 'reading management' and 'monitoring' of consumption. We can notice coherence with Article 13 GDPR and Article 20 f) Internal Market in Electricity Directive.

6.3 Soft law

The EU institutions have also intervened in the topic with instruments of soft law that have clarified crucial aspects of the issue. In 2009 the European Commission set up a Smart Grid Task Force. The goal of the task force was to identify and provide a set of regulatory recommendations. It was divided into three 'Expert groups', where the second (EG2) was tasked with privacy, data protection and cyber-security in the smart grid environment. EG2 sought advice from the Art29 Working Party (Art29WP),[38] which in response produced Opinion 12/2011 on smart metering.[39] EG2 conclusions finally fed into Commission Recommendation 2012/148/EC on preparation for the roll-out of smart metering systems, dated 9 March 2012.[40] The Recommendation encouraged the adoption of a common data

[36] Directive 2012/27/EU of the European Parliament and of the Council of 25 October 2012 on energy efficiency, OJ L 315, 14.11.2012, p. 1–56.
[37] Council Directive 2013/12/EU, Directive 2018/844/EU, Directive 2018/2002/EU, Regulation 2018/1999/EU, see the consolidated version at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02012L0027-20181224, accessed 19 July 2019.
[38] This Body is now called European Data Protection Board. It coordinates and groups Data Protection Supervisory Authorities from the Member States. Like in this case, it might exercise activity of advice for the Commission according to Article 30.1 c) of Directive 95/46/EC.
[39] Art29WP Opinion 12/2011 on Smart metering.
[40] Commission Recommendations 2012/148/EU of 9 March 2012 on preparations for the roll-out of smart metering systems, OJ L 73, 13.3.2012, p. 9–22.

protection impact assessment (DPIA) template and the application of data protection by design and by default. The European Data Protection Supervisor (EDPS) [41] issued an influential Opinion on that Recommendation as well, dated 8 June 2012. The DPIA template was produced by the EG2, but initially it received negative feedback by Art29WP in its Opinion 4/2013.[42] Following further work, a revised version of the template received positive feedback, with some reservations, in Opinion 7/2013.[43] In the end, Commission Recommendation 724/2014/EU suggested the Member States to roll-out smart grids and smart meters in respect of what had been stated by the documents mentioned before in terms of data protection, via the adoption of the final DPIA template.[44] Today, the last version of the DPIA template for smart grid released by EG2 dates back to September 2018.[45]

6.4 Lacunae

Taking into account the EU legislative landscape, some clear gaps can be identified. First of all, there is a lack of a sound and versatile legal basis for detailed consumption data processing. Consent (Article 6.1 a GDPR) would be the most empowering for customers' trust, but relying solely on consent could undermine the efficacy of the smart meter roll-out and of the investments put into place. Indeed, the technology produces the most valuable effects when it is scalable. Contract performance (Article 6.1 b GDPR) is a valid solution for billing purposes, but this legal basis would not justify more frequent data collections than the ordinary billing frequency unless the contract was applying dynamic prices depending on the time of consumption. The legitimate interest (Article 6.1. f GDPR) would play a residual and very volatile role among the contemplated legal bases. For instance, it could be the basis for fraud detection. Arguably, the operation of smart meters does not constitute the accomplishment of vital interest (Article 6.1 d GDPR). If the smart meters were not operating, this would not endanger EU citizens' life, although efficiency and renewable energy success would be negatively affected by such a setback. The link with a vital interest is not so immediate though. Currently, there is no legal obligation (Article 6.1 c GDPR) of carrying on such activity. The last option that is provided by the

[41] The EDPS is an independent Supervisory Authority that ensures that the EU institutions and bodies respect their data protection obligations, as laid down in the EU Data Protection Regulation 45/2001, in force at the time, and now repealed by Regulation 2018/1725/EU. Article 28.2 Regulation 45/2001 reads as follow: "When it adapts a legislative proposal relating to the protection of individuals' rights and freedoms with regard to the processing of personal data, the Commission shall consult the European Data Protection Supervisor".

[42] Art29WP Opinion 4/2013 on the Data Protection Impact Assessment Template for Smart Grid and smart Metering Systems ('DPIA Template') prepared by Expert Group 2 of the Commission's Smart Grid task Force, 22 April 2013, 00678/13/EN WP205.

[43] Art29WP Opinion 7/2013 on the Data Protection Impact Assessment Template for Smart Grid and smart Metering Systems ('DPIA Template') prepared by Expert Group 2 of the Commission's Smart Grid Task Force, 4 December 2013, 2064/13/EN.

[44] Commission Recommendation 2014/724/EU of 10 October 2014 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems, OJ L 300, 18.10.2014, p. 63–68.

[45] Data Protection Impact Assessment Template for Smart Grid and Smart Metering systems, v. 2 of 13 September 2018, Smart Grid Task Force EG2, https://ec.europa.eu/energy/sites/ener/files/documents/dpia_for_publication_2018.pdf, accessed 19July 2019.

GDPR is the public interest or exercise of public authority (Article 6.1 e GDPR), which should be enshrined in an EU or Member State law (Article 6.3 GDPR).

A second criticality is the uncertain attribution of roles among the subjects involved, from the customer to the multiple operators (utilities, DSOs, TSOs, producers, providers of additional services[46]). From the side of the data controller/data processor, all the mentioned entities could have an interest in processing the data coming from the smart meter, but only the ones deciding the means and purposes of data processing will be qualified as the data controllers (Article 4.7 GDPR), holding the corresponding responsibilities and obligations. From the side of the data subject, it is problematic to decide who should be the one exercising the rights: the part of the electricity provision contract, all the single inhabitants of the home or, as a third and last option, the home inhabitants as a whole?

Thirdly, there is not a fixed aggregation threshold, over which the electricity consumption data are considered anonymous. Aggregation is an anonymization method which has already been tested with the electricity data, at least in some states of the U.S.. Colorado and California use the 15/15 rules for aggregation. According to this rule, electricity data referring to at least 15 households, of which none account to a percentage superior to 15%, are not considered personal data anymore, but aggregated data. The threshold is applied differently in other U.S. states, such as Illinois, where it is fixed at least 30 customers.[47] The latter are mere examples, also because the concept of anonymisation in the EU context is quite strict since it coincides almost with the impossibility to identify the data subject behind the data. It would be convenient that a technical group, like the task force mentioned under paragraph 6.3, gave a reasoned suggestion, then endorsed by the lawmaker. The threshold would require to be updated from time to time, following the development of identification techniques. Knowing exactly when personal data are not such anymore after the aggregation would allow for a more agile data processing, especially for subjects such as the TSO or the producers which, in order to maintain the whole grid stable, will not need to know granular data, but just their aggregated form.

6.5 Flemish energy legislation: filling the EU gaps

In order to assess whether some of the gaps in the EU legislation (Section 5.4) have been addressed on the national level, we will take the legislative landscape in Flanders, Belgium, as an example.

In Belgium, the competences regarding energy policy exist on the federal and regional levels. The federal government has competence over matters that require a national approach, such as the transmission of energy and the tariff policy for transmission and distribution system operators. The regions, such as Flanders, have competence over the distribution of electricity and technical aspects of local transmission of electricity through

[46] Pallas, Frank, “Data Protection and Smart Grid Communication – The European Perspective” *IEEE PES Innovative Smart Grid Technologies*, (2012-01), 3.
[47] Mclean, “How Smart is too Smart?”, 899; Harvey, “Smart Meters, Smarter Regulation”, 2090.

grids with a nominal voltage of 70 kV or less.[48] Due to this division of competences, the current analysis will be limited to relevant legislation in the region of Flanders.

In Flanders, the EU Internal Market in Electricity[49] and Energy Efficiency Directive[50] were implemented by amending existing legislation, namely the Energy Decree of 8 May 2009[51] (hereafter 'the Energy Decree') and the Energy Decision of 19 November 2010[52] (hereafter 'the Energy Decision'), which both entered into force in 2011. The Energy Decree serves as the basis for the development of energy policy in Flanders, while the Energy Decision further implements the provisions of the former. The new Internal Market in Electricity Directive[53] and amending Energy Efficiency Directive,[54] as part of the '*Clean energy for all Europeans*' package, will also have to be implemented through amendments.

The first essential element found in the Flemish legislation is the obligation for the Flemish Regulator of the Electricity and Gas market (FREG) to conduct an evaluation of data management activities of network operators every five years. The FREG must also report to the Flemish government every two years on the compliance of network operators with the conditions applicable to their data management activities.[55] These conditions relate, among other elements, to the ability to comply with the requirements of the GDPR in the exercise of data management activities, as well as the ability to respect uniform conditions for a continuous risk management system.[56] The aforementioned data management activities include, among others: the reading of digital, electronic, and analogue meters for specified purposes; the management, processing, securing, and storage of technical, relational, and measurement data; and the provision of necessary data to specified actors.[57]

The Energy Decree also regulates the roll-out and installation of digital meters under Article 4.1.22/2, listing the specific cases in which a digital meter must be placed. Additionally, Articles 4.1.22/4 to 4.1.22/13 regulate the processing of meter data, which could serve as a legal basis for data processing under the GDPR.[58] Firstly, these articles explicitly mention that the data subject retains control over their personal data from digital,

[48] Elia, Legal framework, last accessed on 18 November 2020, https://www.elia.be/en/company/legal-framework.
[49] Directive 2009/72/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in electricity and repealing Directive 2003/54/EC.
[50] Directive 2012/27/EU of the European Parliament and of the Council of 25 October 2012 on energy efficiency.
[51] Decreet van 8 mei 2009 houdende algemene bepalingen betreffende het energiebeleid.
[52] Besluit van 19 november 2010 van de Vlaamse Regering houdende algemene bepalingen over het energiebeleid.
[53] Directive 2019/944/EU of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU.
[54] Directive 2018/2002/EU of the European Parliament and of the Council of 11 December 2018 amending Directive 2012/27/EU on energy efficiency.
[55] Article 3.1.3, 4°, k) and l) of the Energy Decree of 8 May 2009.
[56] Ibid., Article 4.1.4, 2), 5° and 6°.
[57] Ibid., Article 4.1.8/2.
[58] Article 6, 1 (e) of the GDPR; the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

electronic, and analogue meters.[59] Secondly, they further specify the access rights of specific parties to meter data.[60] Thirdly, they state that technical data, relational data, and measurement data may qualify as personal data and determine which actors can be regarded as controllers with regard to the processing of specific types of personal data for specified purposes.[61] The Energy Decision further defines the assignment of legal roles by laying down conditions under which a controller may rely on a processor for the processing of personal data related to their tasks.[62] Finally, the Energy Decree creates an obligation for the relevant parties to establish a continuous risk management system relating to the probability and severity of risks for the rights and freedoms of natural persons.[63] In this context, the Energy Decision obliges specific actors to conduct a data protection impact assessment prior to accessing personal data. Afterwards, continuous risk monitoring should be conducted in order to analyze existing and emerging risks and a data protection impact assessment must be conducted every two years at the minimum. It also includes a list of specific scenarios in which an additional data protection impact assessment must be conducted.[64]

The inclusion of these provisions and accompanying obligations in the Energy Decree and Energy Decision are important steps in the right direction to fill the previously identified gaps in EU law. The Energy Decree establishes a potential legal basis for the processing of smart meter data based on the public interest, which, according to the GDPR, must be laid down and further specified by Union or Member State law.[65] Secondly, the Flemish law better defines the assignment of legal roles in light of the GDPR. Thirdly, the Energy Decree and Energy Decision address the need for a risk management mechanism in several ways. In addition to the establishment of a continuous risk management system and obligation to conduct a DPIA in several scenarios, it also places an evaluation and reporting obligation on the Flemish Regulator for the Electricity and Gas market. One of the identified gaps remains, however, unclear; namely what aggregation threshold should be reached in order to consider personal data fully anonymized.

[59] Article 4.1.22/4 of the Energy Decree of 8 May 2009.
[60] Ibid., Article 4.1.22/5.
[61] Ibid., Articles 4.1.22/6 to 4.1.22/12.
[62] Article 3.1.60 of the Energy Decision of 19 November 2010; this provision lays down the obligation and necessary content for a controller-processor agreement.
[63] Article 4.1.22/13 of the Energy Decree of 8 May 2009.
[64] Article 3.1.61 of the Energy Decision of 19 November 2010.
[65] Article 6, 3 of the GDPR.

7. Where does the technology come in?

The technology provides some tools to preserve privacy (Privacy Enhancement Technologies, PETs). The hook between technology and law is the Data protection by design principle (Article 25 GDPR), which requires that data protection principles are considered since the design phase and hard-wired in the technology. One PET is encryption, which is making the personal data unintelligible without a decryption key. Encryption does not mean anonymisation, at least not for the owner of the key, since for him it would still be possible to decrypt the data and subsequently identify the persons to which the data pertain. In fact, according to the GDPR's definition, encryption is rather classified as pseudonymisation (Article 4.5 GDPR) because it assigns to personal data unintelligible cyphers, which eventually could become intelligible again through the use of other information, such as a decrypting key. On the contrary, proper anonymisation that would allow for the GDPR's non-application, would, in accordance with Article 4.1 and Recital 26 GDPR, render the identification impossible or unreasonably cumbersome to reach. This aspect is often not grasped by the technologies' users, who may tend to think that adopting encryption would per se guarantee anonymity. Developers and operators could fall into this fallacy too, believing that with encryption, all the legal obligations would be fulfilled. Nevertheless, this PET is largely used in other sectors. It is quite known among the public and, even without anonymising, it lower effectively some risks for the privacy of data.

One other PET pertains to the physical dimension instead, through an aggregation of electricity. It consists of the use of a local battery that would inject a constant amount of electricity from the distribution grid and then release the electricity to the home circuit variably, depending on the consumption.[66] In this case, the smart meter would not be able to detect the detailed workload, but rather a constant flow of electricity, from which is not possible to infer the behavioural patterns. The battery solution has the advantage of being easily understandable for the layman and under the control of the customer. While for the adoption of encryption the customer should have to trust, again, the operator. There are a couple of issues for this technique though: (i) Would this PET obstacle the potential of smart meters in terms of benefits? (ii) Who would bear the costs of the battery? These questions require more specific technical knowledge. What can be added from a legal and ethical point of view is that if the costs of the batteries fall upon the customers, this would create a situation where data privacy would be a privilege not affordable for everybody.

8. Conclusions

We have explained that the technology of smart meters brings with it opportunities and risks. The smart meters substitute an old, but functioning technology and the roll-out follows a resolute political momentum with the forecast of a share of 80% smart meters' presence in the immediate future throughout the Member States. It is no surprise that a sentiment of distrust arose due to privacy concerns. In turn, the operators ask for a clear and predictable law. To conciliate the protection for data and privacy and the demands of

[66] Liehuang Zhu, Zijan Zhang and Chang Xu, *Secure and Privacy-Preserving Data Communication in Internet of Things*, (Springer, 2017), 36-37.

operators is not an easy job, but an optimal solution would require the best combination of law and technologies (PETs).

The prolific legislative interventions have tackled multiple issues; general laws were followed by technical studies and opinions by the EU Data protection bodies to further implement data protection norms. We find the EU approach correct, but still not optimal, as missing some relevant aspects that, nevertheless, have almost exhaustively been addressed in the Flemish experience. In our opinion, a trust enhancing law in the matter would fulfil the following requirements. The law should be European for the general principles, but national for the specific requirements, because, despite the admirable will to create a unique EU internal market, the electricity markets are still mostly nationally oriented in the way they are structured and function. The law that we aspire for provides a legal basis under Article 6(e) for the public interest and establishes who the data subject, the data controller and the data processor are in the routine flow of personal data. It specifies which are the 'eligible entities' mentioned in the new Internal Market in Electricity Directive. It introduces the obligation of a Data Protection Impact Assessment (DPIA) according to Article 35 GDPR every time a smart meter is involved, with the exception of the data processing conducted by the households. The DPIA could follow the template already provided (see paragraph 6.3). Finally, based on a technical study, the law sets an aggregation threshold which determines when consumption and production data coming from the smart meters qualify as 'anonymous data', thereby avoiding the application of the GDPR.