Transformations of Trust in Society

A Systematic Review of how Access to Big Data in Energy Systems Challenges Scandinavian Culture

de Godoy, Jaqueline; Otrel-Cass, Kathrin; Toft, Kristian Høyer

Document Version
Final published version

Published in:
Energy and AI

DOI:
10.1016/j.egyai.2021.100079

Publication date:
2021

License
CC BY-NC-ND

Citation for published version (APA):
de Godoy, J., Otrel-Cass, K., & Toft, K. H. (2021). Transformations of Trust in Society: A Systematic Review of how Access to Big Data in Energy Systems Challenges Scandinavian Culture. *Energy and AI*, *5*, Article 100079. https://doi.org/10.1016/j.egyai.2021.100079

Link to publication in CBS Research Portal

Energy and AI 5 (2021) 100079

Contents lists available at ScienceDirect

Energy and AI

journal homepage: www.elsevier.com/locate/egyai

Review

Transformations of trust in society: A systematic review of how access to big data in energy systems challenges Scandinavian culture

Jaqueline de Godoy[a,*], Kathrin Otrel-Cass[b], Kristian Høyer Toft[c]

[a] Aalborg University, Department of Energy Technology, Pontoppidanstræde 111, 9220 Aalborg, Denmark
[b] University of Graz, Institute for Educational Research and Teacher Education, Merangasse 70 / II 8010 Graz, Austria
[c] Copenhagen Business School, Department of Management, Society and Communication, Solbjerg Pl. 3, 2000 Frederiksberg, Denmark

HIGHLIGHTS

- An interdisciplinary and socio-technical perspective to provide a systematic account of the research in big data analytics in the energy sector.
- The article juxtaposes a review of Scandinavian culture of trust and the practices of surveillance capitalism to identify the challenges that big data practices pose for the energy sector.
- Increased surveillance capitalism practices challenge cultures of trust.
- Public's concerns in protecting their privacy are often addressed by focusing on technical improvements.

ARTICLE INFO

Article history:
Received 5 February 2021
Received in revised form 2 April 2021
Accepted 18 April 2021
Available online 28 April 2021

Keywords:
Surveillance capitalism
Smart meters
Energy transition
Trust
Data Ethics
Big Data

ABSTRACT

In the era of information technology and big data, the extraction, commodification, and control of personal information is redefining how people relate and interact. However, the challenges that big data collection and analytics can introduce in trust-based societies, like those of Scandinavia, are not yet understood. For instance, in the energy sector, data generated through smart appliances, like smart metering devices, can have collateral implications for the end-users. In this paper, we present a systematic review of scientific articles indexed in Scopus to identify possible relationships between the practices of collecting, processing, analysing, and using people's data and people's responses to such practices. We contextualise this by looking at research about Scandinavian societies and link this to the academic literature on big data and trust, big data and smart meters, data ethics and the energy sector, surveillance capitalism, and subsequently performing a reflexive thematic analysis. We broadly situate our understanding of culture in this context on the interactions between cognitive norms, material culture, and energy practices. Our analysis identified a number of articles discussing problems and solutions to do with the practices of surveillance capitalism. We also found that research addresses these challenges in different ways. While some research focuses on technological amendments to address users' privacy protection, only few examine the fundamental ethical questions that discuss how big data practices may change societies and increase their vulnerability. The literature suggests that even in highly trusting societies, like the ones found in Scandinavian countries, trust can be undermined and weakened.

1. Introduction

The practices of electronic data-collection and analysis have rapidly spread to several industrial and research fields, producing new types of business models, laws, policies, ethics, and cultural practices [1–3]. The harvesting and processing of data has been claimed to transform how we form our "objects of explanations" [[4], p.12] and redefine how we deal with issues, phenomena, and sets of problems [5]. It is important to clarify what such practices of data collection mean for people in specific contexts for example in the energy sector, where personalised data are being collected through the use of smart meters. The processing of massive datasets (also referred to as big data) gives rise to controversies because of the way personal information is perceived, treated, accessed, and used, and increasingly concerns the public, as identified by privacy scholars, human rights advocates, as well as business organisations [6–8].

Shoshana Zuboff coined the term surveillance capitalism, which is the power exercised through information technologies used to control and modify behaviour, produce revenue, and control markets [9]. This practice follows a logic of accumulation that produces hyperscale assemblies of objective and subjective data about individuals and their habits for the purpose of knowing, controlling, and modifying behaviour and thus, produce new varieties of commodification, monetisation, and control [9]. Big data analysis can show correlations and trends that for example relate to people's activities and preferences [10], and allows

* Corresponding author.
E-mail addresses: jdgo@et.aau.dk (J.d. Godoy), kathrin.otrel-cass@uni-graz.at (K. Otrel-Cass), kht.msc@cbs.dk (K.H. Toft).

https://doi.org/10.1016/j.egyai.2021.100079

target advertising, a practice pioneered by Google though information left by people on their search engines [[1] p.48], [11]. The key concern here is that people leave digital footprints when they are actively online or when their activities (such as energy consumption) are digitally tracked. These footprints provide information to commercially or politically motivated parties, predominantly without their knowledge.

Surveillance schemes can be used to shape civic and democratic choices, reminding us of how far big data mining can go e.g. cases like the privacy violation committed by Cambridge Analytica revealed by public media in March 2018. The company acquired and used data from Facebook user accounts in a mass surveillance scheme, intended to manipulate individual choices in the US Presidential election of 2016 [12,10]. This exemplifies the impact to the public trust when their fears are confirmed that their vulnerability in what data they produce electronically has been betrayed.

This tension between trust and degrees of vulnerabilities in a datafied society, raise several concerns that are best examined by focusing on a selected topic. In this article we want to contextualise these concerns by focusing on the use of smart meters in the energy sector with the following questions: first, who has control over data? Should it be restricted to only those who have the material, cognitive, and financial resources to access and process big data [14], so that they can potentially make unauthorised decisions on behalf of others? Second, how does big data harvesting, analysis, and processing challenge the concept of trust within societies? Simon [15 p.154] points out that we move and act within highly entangled socio-technical epistemic systems and need to decide when and whom to trust, when to withhold trust, and when to remain vigilant. Third, since the literature found in our database on big data and smart meters is mostly focused on addressing technical issues, it leaves a clear need to identify other underlying dimensions between people's trust and procedures like smart metre systems and data processing technology [7,16]. In comparison, in fields like education or health, the discussions on data processing and mining have increased, for example in the context of children's education by Lupton and Williamson [17]; or how hyperconnected health systems impact peoples's lives [18]).

In the energy sector, the collection of peoples' energy consumption data is being normalised through the wide-spread installations of smart grid infrastructures. However, little attention is being paid to how the collection and management of energy use data shapes people's behaviour [5,14], how data is being used for profitable purposes [13], what kind of private information is being collected in peoples' houses through smart meters [19], or how digitalisation impacts human relationships. Such lack of clarity on how energy consumers' data are managed and processed could potentially lead to controversies, confusion, and misunderstandings potentially threatening the transitioning process towards sustainable energy consumption. In this article we investigate the use of smart meters in the energy sector as an example of a technology that allows such practices. We focus on smart meters since they represent technology that collects private information and increases people's vulnerability since people have to entrust their data to a third party. In the article we will also refer to other technologies that imply similar potential threats as smart metre data do through the processing of data.

The advanced metering infrastructure (AMI), referred to as "smart meters", measures and records energy usage data with temporal and power resolution precision, making consumption information available to the user as well as to the energy company that is connected to the device [2]. Such technologies are said to be utilised for monitoring and maintaining the electricity grid e.g. for detection of faults or energy losses, as well as for demand response and time variation of energy prices [2]. Besides, it is claimed that this helps to manage the intermittency of renewables (like wind and solar) through the management of supply-demand. However, the public is increasingly suspicious about data-gathering technologies, due to growing concerns about possible privacy violations [20,21] and other ethical issues, given that energy consumption, but also personal information related to consumption, can be gathered or inferred through smart meters [2]. Furthermore, the collected data could potentially be sold to third parties and used to shape peoples' future energy consumption behaviour without any consent on their part.

Clarification is not only needed on the potential use of data, but also on the actual uses of data analytics in the energy sector, including what kind of mechanisms are being developed for privacy protection, and if surveillance capitalism practices tend to proliferate. Data collection could take place in a covert way, where the user is kept in the dark about the kind of data that is being collected (e.g. geolocation information from cell phones) [22]. In fact, Birchall [22] points out that there seems to be a widespread major misunderstanding as to what the concept of data 'sharing' entails, since sharing implies reciprocity and openness. When permission to collect data has been given, the terms and conditions of data protection that users sign are often ambiguous and not necessarily specific enough about how and what data will be used for [20]. In many cases the general public is informed that the change to smart metre systems will take place with little or no information to what data is being collected and how it is being used. Thus, heightened awareness of the potential risks of surveillance capitalism in the energy sector could mitigate infringements of energy users' right to privacy. The issue is that the more opaque the details about this kind of data processing are kept, the greater the chance that the public will be susceptible to believing in 'alternative facts'. Since transparency is a fundamental principle in the General Data Protection Regulation (in Art. 5(1)(a) of the GDPR, see also [23]) it may also heighten the chance that decision makers have more trust in the accuracy of such analyses [24].

Social trust is needed in the push for the decarbonisation of the energy sector, since transitions towards more sustainable futures will require the cooperation of all stakeholders including between citizens and institutions [25–27]. However, there is a lack of research on what precisely is meant by a societal trust in big data technologies, since trust is relative to and shaped by cultural settings, societal influences, and context [21]. It would therefore seem very relevant to get a better understanding of how to enable trust by means of the management of energy consumption data.

To further such insights and understandings, in this article we review how big data is reported to be used in the energy sector, juxtaposed with a review of the literature on trustworthy cultures as well as the topic surveillance capitalism. We thus examine the potential challenges energy surveillance capitalism can have in the context of Scandinavia (which in this paper refers to Norway, Finland, Sweden, and Denmark). Our interest in Scandinavian countries is twofold: first, these societies are characterised by high levels of citizens' trust in both public and private institutions [28]. Second, because we, the authors, are participating in an interdisciplinary EU Horizon funded project on Energy Transition of the North Sea Region (ENSYSTRA). The primary aim of this work was to identify possible correlations between surveillance capitalism practices, Scandinavian culture of trust, and data processing practices in the energy sector.

Smart meters are hailed as a primordial step towards a low carbon economy [19] but have implications for householders, since people's data is automatically measured and automatic adjustments can be made to regulate people's energy consumption [29]. In some countries, the introduction of smart meters has met public resistance (e.g. in the Netherlands [30] and France [31]), mostly because of questions over privacy issues and the lack of democratic legitimacy. Critical voices have pointed out that this is due to a lack of both open communication and public involvement in the decision-making processes, which indicates a lack of institutional trustworthiness [29]. The roll-out of smart meters devices in Scandinavian households started in 2003 with constituent countries adopting similar approaches for smart meters installation, ownership, and storage of data. For instance, the collected data is stored in a central hub and its stewardship is the responsibility of the distribution system operators (DSOs) [32,33]. Evaluation of the functionalities of the smart meters was carried out in Sweden. The regulatory authority for energy markets decided that improvements are required to meet some minimal functions (like modifying the customer interface) to make the consumers more active in energy-saving and manage the consumers' energy behaviour as it is intended for [33]. Furthermore, issues related to data security should be resolved. Interestingly, privacy protection was not considered amongst the essential requirements, according to Huang [33].

Early on in the ENSYSTRA project, we conducted a literature synthesis with an interdisciplinary perspective [34] and observed a lack of socio-technical and ethics research on the topic of big data in the energy sector. Thus, we decided to approach the review by collecting and processing the dataset as a body of social-technical information to learn what detailed information such processes reveal [35]. Hence, the work that is presented here presents a focused and systematic state-of-the-art review. Our attention on trust and surveillance capitalism required tapping into different disciplinary fields to then imply where we see connections. To explore possible correlations, we identified key terms used in scientific articles and examine the main methodological instruments that were used. We also included work that examined surveillance issues for larger populations and what this implies for individuals [36]. Since we are examining research that seeks to explore people's trust in smart metre processing, we need to also position ourselves how we interpret culture, specifically in respect to energy practices. For that purpose we found the energy cultures framework a useful underpinning which highlights a tripartite between material culture, practices and norms [37]. Stephenson et al. [37 p.118] write: "A subject's energy culture may be partially self-determined, but is likely also to be shaped by external influences that are beyond their direct control." With this in mind, we are aware that people's trust in adopting smart metre technology and data processing may be shaped by a number of factors including also migratory factors or people's socio-economic situations. We made a decision not to dive into norms or practice-orientated topics that explore, in particular, how individuals enact things day-to-day, but rather explore the research that examines material cultures, since this dimension is heavily interwoven with norms and practices and examines people's choices in materials that are driven by implicit meanings [37,38]. Since systematic literature reviews are also very resource intensive activities we made a decision to adopt this focus. However, we are aware that those factors, as well as external aspects (particular circumstances such as migration), also shape people's perception of who to trust.

In the following section, we will explain the process of analysis of relevant literature to answer the research questions above.

2. Methodology for the systematic literature review

We intend to make this review replicable and traceable since we want to go beyond a narrative presentation of our findings from the literature [39]. For this reason, we started with a systematic literature review (SLR) approach [40] followed by a reflexive thematic analysis [41,42]. In the SLR, our focus is on the journal output, and the methods researchers' have used. Once articles of relevance were identified, their findings were summarised based on defined criteria (Table 2). We also followed the guidelines of Keele [43] for the planning, conducting, and reporting in a literature review. However, the stages were slightly adapted for our study, as shown in Fig. 1.

We used the Scopus database because it represents a complete source of quality research. Since we aimed to provide a broad cross-disciplinary review and in-depth synthesis from relevant areas of social sciences, life sciences, physical sciences, and health sciences, we did not restrict our analysis to article types, also including book chapters and peer-reviewed articles presented at conferences. However, some sources like reports or government documents were excluded. Once bibliographical resources were identified, we needed to make sense of this knowledge corpus and thematically organise the findings. By utilising reflexive thematic analysis [44], we were able to identify patterns which defined key themes represented by the selected clusters of articles. Since the keyword selection for the database search was a significant step, we present how we identified keywords next.

2.1. Identification of keywords and review process

As a first step, we identified key search terms. We started with the words "Surveillance" AND "Capitalism" AND "Energy" AND "Sector" as well as "Surveillance" AND "Capitalism" AND "Trust". However, this search generated very few results, we found no articles with the combination of surveillance capitalism and the energy sector, and the keywords surveillance capitalism and trust produced only five articles. However, this initial investigation confirmed our suspicion for the need for a more refined search.

We continued our search with keywords based on Zuboff[14]'s article, where the term surveillance capitalism was coined. To our knowledge, Zuboff [14] was the first to associate the theme of a surveillance practice with the issue concerning big data. Although surveillance capitalism can have a normative description, it is an object-phenomena practice in contemporary computing [45]. Surveillance capitalism demands investigation of the entanglements of laws and regulations that ought to guarantee users' rights of privacy while identifying the benefits of big data processing for the energy sector that guide this development. The search strings were created using the Boolean AND, according to the keywords described in Table 1. The table shows the terms used in the search, as well as the number of articles found. First, we traced the connections that surveillance capitalism and big data have with energy technologies in the context of smart systems and the smart metering apparatus. Second, we reviewed what the literature says about data ethics and how this can challenge the level of trust that societies have in institutions when surveillance capitalism is carried out by these institutions. Our methodology for the paper selection is summarised in Table 2. The first search was conducted on November of 2019. However, we updated the dataset with a new search on August 2020.

In the following section, we present the qualitative analysis of the articles, along with their central claims and the methods used to make such claims.

3. Results

Our analysis resulted in the identification of five topics: surveillance capitalism, trust culture in Scandinavia, trust in big data, big data in the energy sector, and data ethics in the energy sector. The themes, numbers of articles for each topic, as well as the authors and respective methods they used, can be seen in Tables 3–7 of the Appendix.

3.1. Surveillance capitalism

Topic one was "surveillance capitalism" (Table 3 of the Appendix) and has seven themes: control, privacy, cultural impact, business models, market sectors, smart technologies, and general data protection regulation (GDPR).

We followed Zuboff's [14] definition of surveillance capitalism as emergent architecture for data processing and analysis that creates new markets with the logic of monetising and controlling behaviour, where "hyper-scale assemblages of subjective and objective data about individuals and their habits" allow to monitor or modify peoples' behaviour [4 p.85]. Here, control naturally appears as a theme, and we observed that authors connect the architecture [14,36] behind surveillance capitalism and the mechanisms used for data processing to describe it as a form of control: personal, bureaucratic and social [46]. Exerted by monopoly organisations [47] in which the government plays the role of creating the surveillance infrastructure [48]. This has implications for individuals [49], society [47,50], business models [48,51,52] and policies [51,53], e.g. how the deliberate control through data processing architectures influences people's behaviour, thus reducing individual's

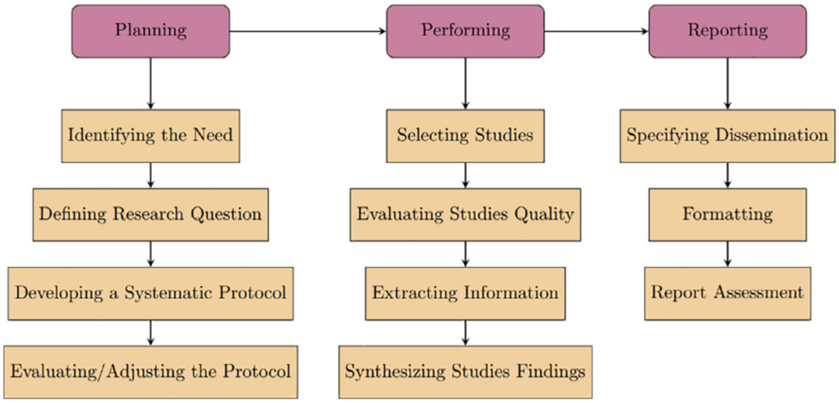
Planning
Performing
Reporting
Identifying the Need
Defining Research Question
Developing a Systematic Protocol
Evaluating/Adjusting the Protocol
Selecting Studies
Evaluating Studies Quality
Extracting Information
Synthesizing Studies Findings
Specifying Dissemination
Formatting
Report Assessment

Fig. 1. Adopted methodology for systematic review, adapted from Keele [43].

Table 1
Specifications of the search terms used in Scopus updated on 05.08.2020.

Keywords strived in the Scopus database	Total of articles found	Period of the articles	Remaining articles (after steps 2 and 3, Table 2)	Analysed articles
"Surveillance Capitalism"	80	2014 - 2020	39	30
Scandinavia* AND Culture AND Trust / Scandinavia* AND Trust	28/269	1998 - 2020	6/21	26
"Big Data" AND "Trust"	1.053	2011 - 2020	161	42
"Big Data" AND "Smart Meters"	293	2012 - 2020	37	26
Data AND Ethics AND Energy AND Sector	12	2011 - 2020	4	4
Total				128

Table 2
Criteria of inclusion and exclusion of the bibliographic resources.

Criteria	Details
Languages considered	English, Spanish, Danish, German, Portuguese, Swedish. However, most articles were English.
Collected information	Focus on the key statements, general aims and research instruments (theoretical and methodological).
Article selection	Step 1, initial search terms, according to Table 1: 1. "Surveillance Capitalism"; 2. Scandinavia* AND Culture AND Trust; 3. "Big Data" AND "Trust" and 4. Data AND Ethics AND Energy AND Sector. 5. Big Data AND "Smart Meters". Step 2, was for the determination of the suitability of article focus (reading of title, abstract, results). Articles with an unrelated focus to our research question were excluded. Step 3, the selected articles were examined using the following questions: 1. Is the article exploring the origins, consequences or characteristics of the corresponding area? 2. Is one of our key areas a focus central to the paper? 3. Does the aim of the study allude to insights for our study? Step 4, assessment of reliability and validity of the studies: 1. Do the studies follow a rigorous and scientific method to reach conclusions? 2. Are the studies supported by a rigorous methodology that supports the findings? 3. Do the authors offer enough information to verify the accuracy of their study?
Thematic analysis	128 articles were analysed. Articles that fitted more than one thematic code were assigned to the code that fitted the general intention of the article.

ability to think and make choices [49]. Significant here, is that the literature already indicates how the ideologies behind the control through data insights impacts on societies' practices and disregard their human culture [54] and presents a potential threat to individual's privacy [54–56] (e.g. Internet of things (IoT) [54] or speech recognition systems that are embedded in smart home appliances and can capture and process people's conversations [55]).

"Surveillance culture", as discussed by Partin article [57], are also impacting human agency in networked systems and may create data injustice when the production of big data results in discriminatory treatment or representations of individuals or groups [54,57,58]. The "digital surveillance economy" operates with business models that place corporate interests at the centre, threatening individuals, societies, and policies due practices of manipulation of consumer's behaviour, cross-correlation of personal information in favour of target advertisers, consequently accumulating wealth by the commodification of human behaviour [59–62]. Such market logic aimed at profit has consequences on the health of users of social media, like depression and anxiety, and also blurs and resignifies the notions of private information [61] and outsmarting users (due to e.g. the power given to semi-autonomous intelligent personal assistants where users are unaware when their privacy is compromised [55]).

Furthermore, Barassi analyses the structure of business models based on market commodification and user profiling arguing that there is systematic coercion transforming citizens to "datafied citizens" as we are induced to act in favour of other actors, giving up our data that till now was considered private [13 p.415]. The concern with surveillance capitalism practices becomes pertinent when we see how these are spreading across several market sectors. In this regard, several articles examine human experiences when users are positioned as objects for data-generation (e.g. children apps [63], pregnancy apps, parenting apps, IoToy [64], fitness appliances [65], or dating platforms [66]).

Concerning smart technologies, a set of papers also focus on the ideologies underpinning those technologies. For instance, in urban governance there is a tendency of framing urban problems as of technological origin, turning those spaces into digitalised infrastructures and as an engine for urban economies [67]. Thus, cities and people's houses [68], are becoming a ready platform for surveillance practices for example with the spread of Intelligent Personal Assistants (IPA's) and sensors being connected to social media. An effect observed on users is the deprivation of conscious agency and the increased tolerance to such practices [69].

Further, due to the potential threats surveillance practices present to the protection of people's privacy and data, the General Data Protection Regulation (GDPR) came into force in Europe on the 25th of May 2018. Since then, many studies focused on understanding the mechanisms, principles, social and economic implications and operations of this regulation [70–72]. Amongst the approaches proposed in the literature for protecting people's privacy are anonymisation, pseudonymisation, right to be forgotten, and the right to withdraw collected data and one's participation. However, discrepancies are reported on how these regulations ought to work and how are they applied in practice. For example, an app in the healthcare sector may include an opt-out possibility, but if it is too complicated for users to unsubscribe from or uninstall, it remains a case of infringement on people's rights of privacy protection [72].

3.2. Trust in Scandinavian cultures

In our search on the Scandinavian culture of trust, the keywords "Scandinavian Trust" and "Scandinavian Culture of Trust" resulted in the identification of seven themes: Economic development; control; institutional trust; interpersonal trust (social trust); ethics; social and environmental responsibility; and digital trust. The papers under each theme and the methodology they applied is described in Table 4 of the Appendix.

Scandinavia is known for having a high level of trust between citizens and in the institutions. The origins of this cultural trace appear to be historical ancestry roots, mostly due to the way long-distance trade was made in the Viking age [73]. At that time, trade between strangers was guided by informal oral agreement. Thus it required trust to deal with risks of potential frauds and due to the absence of written documents [73]. Nowadays, this Scandinavian culture of trust still has an effect on socio-economic success, since, for business developed innovations, it is key to have a cooperative relationship between e.g. customer and service companies [74]. However, the relation of trust with control has been the subject of intense debate. Notably, the decline in political trust in Norway [75] has been connected with the abundance of natural resources (oil wealth). Distrust arises about who has control and how Norway's wealth of resources is distributed, leading to a divergence of interests between voters and politicians [75]. Lueg [76] investigated the effects of control when alliances are being formed in the financial services industry, concluding that control can have ambivalent meaning for the parties involved and can be a threat to the goodwill of trust between those involved, harming mutual trust, delaying, or impeding the negotiations to form alliances.

Many studies in our dataset explored the nature of trust as a core value of Scandinavian institutions, focusing on understanding the principles followed by public institutions [77,78]. Trust is a well-known characteristic of the functioning of science and innovation research projects [79] and for increasing civic participation in democratic governments [80,81]. It plays a role in the engaging of individuals to cooperate in group activities (conceptually known as "social capital"). For instance, in the building of relationships between governments and voluntary organisations [81,82] and in the pursuit to increase transparency and helping to avoid corruption [83]. Societies with institutions that can be trusted are reported to have more community resilience [82] and have an increased ability to finding solutions during recovery from economic crisis (e.g. by helping build citizens' resilience, creating new educational or training programs [84]).

Scandinavian social trust is also characterised through interpersonal trust. Comparisons amongst 29 European countries show that Scandinavian countries have the highest individual levels of social trust and that those societies share similar values [28,85]. Those shared values are related to the high level of social capital and correlated with low levels of corruption, economic equality, and non-discriminatory systems [81], boosting a cooperative behaviour on people [28]. Sjoberg [86] studied the role social trust plays in Sweden in the prevention of risk situations e.g. in the context of nuclear fuels. The authors conclude that in this case, social trust is less important than epistemic trust (the trust in science and technology per se). This highlights that different types of interpersonal trust exist in Scandinavian countries that lead to different behaviour [87]. For example, Gulbrandsen [88] argues that the e.g. Nordic elites and top leaders have more trust in institutions and in the system than their citizens. Mostly because elites of a society tend do drive how such institutions work (e.g. they are involved in large networks of influences) thus, they have more knowledge about such decisions than the general public and are able to discern when it is possible to trust or not in a specific system [88]. Besides, in Scandinavia there is a tendency to trust in institutions (private or public) because, business representatives from e.g. Denmark have their ethical values grounded in trust, transparency, and integrity [89].

This can also be in favour of incorporation of sustainability practices and corporate social responsibility, since there is a relation of trust with participation and environmental responsibility [90]. The connection between trust and Scandinavian corporate social responsibility is argued to be based on a trust relationship with e.g. the supply chain from foreign countries, resulting in a corporate advantage for businesses [91]. Countries immersed in a trust culture have more local participation in nature conservation projects [90] and awareness regarding energy policies (i.e. environmental attitudes, self-reported electricity saving behaviour [92]). One example that reflects the positive influences of trust is the case of local support for nuclear waste disposal in Sweden [93,94]. They reached a level of consensus on acceptability, mostly due to how the risk of disposing of nuclear waste is perceived associated with a high level of trust between society and government. Reciprocal trust was enhanced through public participation in intense discussions (at political, media and the public) as well as open public consultations to strengthening resilient democratic institutions that reach a high level of consensus [93,94].

Related to digital technologies, high levels of social and institutional trust present in Scandinavia tends to be a cooperative advantage since citizens accept the sharing of data deposited at biobanks and also show acceptance of digital services. Lack of trust, in this case, has been pointed out as a barrier for consumers' acceptance of e-commerce and internet banking practices [95]. In Scandinavian countries for example, citizens are generally supportive of sharing their health data on large databases (see, for instance, Andreassen's study in psychiatry [96]). The openness of the population is mostly due to the trust in the institutions that handle patients' data, and this is beneficial for the development of e.g. biomedical research. However, ethical standards should exist to guarantee digital data management of sensitive information like people's health data. Furthermore, citizens' perception of how trustworthy an institution is when handling their data is determinant of whether the institution succeeds [97].

3.3. Big data and trust

Under the search term "big data AND trust" we identified seven themes: datafication, dataveillance and surveillance; privacy and security; philosophy, ideologies and ethics; people's behaviour; governance; General Data Protection Regulation; smart technologies. The main themes, number of articles for each theme, as well as the author and respective methods used, can be found in Table 5 of the Appendix.

In some populations like that of Sweden, concerns are rising due to the risk of datafication, dataveillance, and surveillance [98]. According to Van Dijck [99], dataveillance is the continuous monitoring of metadata for an unstated present purpose. This is in contrast with surveillance, where monitoring is done for a specific purpose. Most of the Swedish population are reported to having a negative attitude towards corporations collecting their data, but paradoxically users' remain permissive towards such practices [98]. For instance, users keep sharing data without making a great effort to protect their privacy. This is partially reinforced by the perception that surveillance on the internet is a prerequisite for accessing the benefits from the service provides [98]. Overall, the concern is indicating the erosion of the social foundation of trust, after an observed decrease in trust towards all public institutions who collect data, even when it is done for research purposes [99]. Several solutions to protect from privacy violations are under development with an emphasis on the need for incorporating "privacy by design" when developing big data applications [100]. Although surveillance associated with big data may have partial benefits, like the capability of preventing the spreading of diseases, ambivalences exist about the implications of sharing the required personal information [101]. Hence, citizens are often suspicious about governments controlling their health data, leading to changes in attitude towards data collection technologies [101]. In this manner, nontechnological trust-centric approaches like transparency, control, open dialogue and ethical frameworks could build public trust and help to reach a critical consensus that takes into account the context in which data is collected [102]. Furthermore, there are security and privacy challenges dependant on the underlying big data infrastructures for data collection and analytics that require improvements in the traditional technology approaches, in terms of efficient encryption and decryption algorithms, privacy preservation mechanisms, reliability [103], and of the 5V's characteristics of big data (value, variety, volume, velocity and veracity) [104]. The privacy problem rely on the amount of personal information can be known by others [102].

When it comes to the ethics of big data-related activities, the literature acknowledges epistemological and ontological challenges, as well as those regarding the transparency, reproducibility, and reliability of the data. These concerns lead to actions like the creation of The Council for Big data, Ethics and Society in the US to help maintaining public trust on social data management [105] (for an example of generation of official statistics in UK see [106]). Fundamentally, ethical questions for social scientists involve power relations that, when relying on data, can favour or exclude groups or the data used to inform policy-decision making can lead to misleading choices [107] or lead to partially informed decisions due to the big data automation techniques [108]. Overall, the literature suggests that decisions that are driven by big data should be combined with qualitative methods (e.g. storytelling), to include humans' perceptions of reality [108]. An inclusion of translational data science should support explaining the results to avoid that people trust black boxes that data science can represent to them [109]. There is a consensus about the need for maintaining public trust over decisions made based on big data. In this regards, it is argued that there is a potential that big data impacts people's freedom to make life decisions [110]. However, opposing views argue that the purpose in which algorithms are created is for e.g. companies own interest, thus having a very specific focus. On the other hand, decisions humans face are so unique in each life situation that users are unlikely to be able to rely completely on automation technologies to make personal decisions. Clarification is needed of what trust means in relation to decision-making relying upon big data, and the complex relationship between consent, trust, and justice (e.g. see bioethics research) [111].

Articles exploring people's behaviour towards trusting big data, mostly focus on the agency of algorithms, the perceptions of different groups, and how consumers and users of digital technologies are adapting to it. How well organisations integrate big data into their processes is influenced by the perception and attitudes towards big data by corporate managers [112]. Strategies can be adopted to stimulate organisations trusting in data, like monitoring the insights that support decision-making, understanding the limitations of big data analytics, and the ethical and social issues of relying on big data for decision-making [112]. A trust crisis in big data technologies have already been identified e.g. in China that lead to providing false personal information or a refusal to share data [113]. Privacy boundary management [114] tools support at an individual level [115], the factors influencing under which circumstances people voluntarily provide data. Influencing factors may include gender, educational background, age, perceived benefit by the public, and the purpose in which data is being collected [113,116]. Besides, users' knowledge about ubiquity technologies, the business strategies using big data technologies [117], and a sense of security and privacy are factors influencing consumers' willingness to leave their digital footprint [114]. Likewise, factors identified that tied trust relationships between users' organisations and data technologies are associated with the company's business strategy [117], the control users have over data provided (e.g. social media platform), and the perceived risk and trust consumers have in the services [114].

Some authors focus on how data is driving changes in governance, highlights are being given on big data as evidence for decision-making, and as a form of governance itself. The articles analysed focus on the trustworthiness and quality of datasets being used to inform policy decisions [118], to the automation of urban spaces [119], and the need for strategies that build trust while also guaranteing citizens' privacy and data quality [118]. To Rieder [119], additional insights can emerge from examining social, political, technological, and epistemic roots as big data is starting to be seen more than a black box and data validity is worthy of contestation [119]. In this regard, appropriate management of big data should be carried out in order to guarantee compliance with the laws and regulations towards citizens' privacy-protection, when using the internet-of-things by collecting citizens' data through the sensors in the urban environment [118] and in e-governance, for instance [120]. Accountability of performed actions with data collected and users' participation to validate proposed solutions in governance can guarantee citizens' trust in public services [120], enhancing cooperation, and increasing trust between citizens and organisations about the purpose of data collection. Intentions for data collection vary, the private sector's expert focus on perceived benefits, while the public sector's experts considered trust, investment, perceived costs, and relationships as the most important factors in shaping the information-sharing arrangement between public and private [121].

Articles that focus on GDPR analyse and compare European countries' adaptations to the new regulations. Variations rely on the role played by governments, civil rights organisations, and authorities for data protection. Concepts like privacy impact assessment, privacy by design are emerging in some countries where the debate about data protection are more intense [122]. The literature also shows the development of tools like the personal data management systems (PDMS) [123] and Data Track to enforce compliance of the GDPR rules and increase the data transparency, respectively [124], and to manage marketing activities in virtual private shopping assistants (VPAs) [125].

Big data applications strongly rely on the development of smart technologies. Furthermore, transformations of society generated by smart technologies will change how official statistics are generated, bringing up practical and political questions [126]. For instance, how do we deal with anonymity and consent required for data collection according to the GDPR regulation, and how do we include citizens as they become co-producers of statistical data [126]. Hence, articles concerned with respecting individuals' privacy meanwhile implementing and developing "smart cities" look at the design of tools for data collection [127] and technologies like cognitive sensors that have been implemented in cities in Northern Europe [128].

Such practices should allow for privacy, security, transparency, and maintaining citizens' trust in data usage technologies while providing the benefits and functionalities offered through big data use. One method proposed in the literature involving citizens in decision-making is through the use of dashboards; giving an account of the data being collected and allowing the development of both smart cities and smart users. Amongst the challenges of dashboards is proper design in order to avoid misinterpretation or lack understanding of the data [129]. Furthermore, urban environments are susceptible to data-driven nudges, meaning that data collected can be used for profiling purposes [130]. Thus, ethical and legal considerations should assist the implementation of practices linked to the smart cities concept to avoid interfering with the trust that citizens have in institutions or in the government [130].

Trust is one of the top issues for the usage and development of applications of smart technologies, and some interesting cases on new applications concerned voice command devices [131], smart farming [132], and water networks [133], which all have their raft of privacy issues. Trust is fundamental at a housing level due to the range of detailed personal information smart devices can access. For instance, voice command devices (VCD), such as Amazon echo, can access a range of detailed personal information through schedulers recognising user meeting's details like who the participants are, the time and location, as well as individuals sleeping and physical activity patterns [131]. Interestingly though, some findings show how individuals adopt practices that ensure increased privacy protection e.g. by creating new accounts to use the VCD instead of linking those with the details of existing accounts [131]. While control over private information is seen as a societal problem, finding solutions is argued to go beyond the individual level [98].

The smart farming sector's development requires relationships of trust amongst the stakeholders for aligning opportunities, enhancing cooperation between partners, and the automation process [132]. As an early-stage sector development, it was recommended to focus on building the capability of growers and farm businesses to deal with data technologies. Thus, farmers can be data consumers and co-creators of data [132]. Furthermore, smart technologies have the potential for water management. For instance, smart metering infrastructure coupled in the water infrastructure plays a role in improving metre reading accuracy, the knowledge about peak demand and is seen as a social benefit because it improves the customer's engagement helping to build trust relationships [133].

Smart environments with the development of IoT have a considerable challenge of maintaining users' trust, about data gathering technologies, ubiquitous computing, and artificial intelligence development. All articles recognise IoT's security challenges, smart environments, smart cities, and blockchain technologies [134]. Some articles focus on developing technological solutions to certain issues, like the abuse of privacy and the unauthorised access of information, that are amongst the risks identified with the internet-of-things and smart environments [135]. Solutions context-wise try to ensure the privacy in smart environments and IoT, for instance, when sharing patients data with the same disease approaches like anonymisation techniques with random sampling approaches exist however, limitations like the loss of details are present and do not guarantee safety when sharing user's data [136]. Furthermore, attempts are being made to guarantee secure energy demand-side management through IoT management [137].

Clearly, the collection of data is changing the way humans interact with their environment. And further developments of IoT applied in smart grids can influence even more due to the fact that information collected in the "physical" world needs to be confirmed with the digital information from users. Thus in order to develop the technology, users need to participate more actively [138]. One article specifically analyse data from the smart meters to establishing trust levels between decentralized substations by e.g. detecting abnormal behaviour on the data, using techniques like machine learning and static methods [139].

3.4. Big data in the energy sector

Topic three was "Big Data" AND "Smart Meters". Under this topic, we identified five sub-categories: energy data analytics, data-based applications, market research, security, and privacy. The main themes, number of articles for each theme, and the author and respective methodology used can be found in Table 6 of the Appendix.

Analytics on smart metre data promises efficiency improvements across the electricity grids by dealing with the challenge of integrating renewables resources into the power grid, that require balancing supply and demand loads, which bring technical challenges like reliability, economic and flexibility (REF) [140]. Data analytics techniques in development are for load analysis, forecast, and management of energy systems and for providing personalised consumer services [140]. The raw data required for the analysis was derived from the demand sides, generally consisting of private information, collected from smart meters and appliances [141]. Thus, one of the core discussions of data analytics on smart metre data is privacy issues due to inference of socio-demographic information from users. Ethics questions related to user's privacy and data security remain, and are not fully understood. Some questions are for instance, "who owns the smart metre data?, and how much can private information be mined from these data?" [135 p.291].

The advancement of techniques for data collection and processing is mostly occurring due to a lack of regulation on the power industry [142], disregarding the "highly secret" characteristic of the information collected from consumers [143]. That, is of two types: energy consumption and abnormal events on the grid [143], collected with a time-precision of every 5 to 15 min [144]. Data analytics techniques in development are using synthetic residential loads to prevent customers' privacy leakage [145]. For example, synthetic data from electricity from buildings can be generated (based on factors like type and building quality, occupation type [145]). However, such datasets will need to be validated with real data from buildings [145] that make it unlikely that users' privacy will be protected. Furthermore, data analytics on residential electricity consumption normalise technics for population segmentation, and the "end purpose of smart metre data is to generate insights into societal trends and behaviour" [141 p.11]. This is done by using statistical machine learning frameworks (Gaussian mixture models) to cluster energy profiles (in the form of time-series). However, they claim that their approach enables targeting and prediction of energy consumption while keeping the anonymity of individual profiles for the customer [146]. Other studies focus on energy management by allowing utilities and consumers to process and validate real-time energy consumption acquired from smart houses by methods of unified fog computing architecture [147].

The mechanism of data analytics itself couple socio-demographics, socio-economic, dwelling characteristics, and occupant energy consumption behaviour to consumer segmentation improves prediction and analysis of the grid (such as peak load prediction, tariff plans and theft detection) improve demand response and energy savings [148]. Also, for identification of anomalous energy consumption, by clustering smart meters' data and looking for deviations in statistical measures [149]. However, the success of increasing energy efficiency depends highly on the customer's willingness to adjust their behaviour. The problem relies on the fact that individuals private information is in possession of other parties. The benefits of having energy data available are for research that can inform policy-makers, improve products and services, accelerate the development of demand-side technologies, and for the creation of energy policies that shape consumers' attitudes and behaviours [150]. Furthermore, data can also be used to detect anomalous energy consumption like faults, losses, or energy theft [150].

Similarly, techniques use segmentation analysis of consumers and clustering of smart buildings' data for spacio-temporal energy profiling and prediction, categorising the consumers' electricity and water usage into different levels [151, 152]. Furthermore, advancements in data collection and analyses also enable novel forensic techniques, where evidence can be recovered from smart home appliances and server files (e.g. see the framework for forensic acquisition and analysis from smart home automation systems (HAS) developed). This is one example of a dual-use problem [153] of having householders data collection.

Market research papers deal with business models' characteristics behind smart metre appliances, customers, and stakeholder decision-making processes. The groups benefited by smart meters deployment identified are the energy distributor, the consumers, and the retailer (energy supplier). The energy distributor can benefit from having accurate consumption data, helping to e.g. detect faults or energy theft. For the consumers the benefits are on the increasing the awareness of energy consumption at e.g. appliance levels. Moreover, the retailers benefit from "understand and profile customers for target services for better loyalty" [149 p.428]. For the functionality of this market, all stakeholders should collaborate. However, trust in the utility companies and the need for privacy and security improvements were reported as a societal barrier for smart home appliances to penetrate Germany's marketplace. Furthermore, smart meters do no guarantee energy savings by the current legal-framework [155]. Even so, authors propose a credit-based system to motivate customers to share private information for industrial and economic purposes [156].

The security challenge is also tackled in the literature reviewed. Databases can suffer attacks, manipulation, and falsification of data. They are representing a pressing security issue for energy systems and data analytics. Technics in development for security defence in power grids exist, like the use of deep belief network for detecting false data injection [157] and for analysis of non-technical losses e.g. detection of energy theft [158]. They do so by comparing consumption data from the smart meters to identify discrepancies (through multiple linear regression) [158]. Such research is relevant and directly applicable to the IT and IoT infrastructures underlying smart grids. Furthermore, research on cryptography applied to energy systems aims to protect sensitive information towards unauthorised attacks by designing encryption schemes that protect, store, and transfer user information [159].

The monitoring of electricity consumption carries the risk of revealing personal information. Although real-time electricity consumption data may be collected for energy management, the consumers' routine can be inferred from postprocessing such data. Thus, privacy preservation techniques are required. Most of the articles relating to privacy develop and evaluate computational models or frameworks for privacy-preservation using e.g. lightweight cryptography or aggregation of smart metering data. Methods in development to preserve users' privacy focus on minimising the information provided by smart meters e.g. when a battery is available to the smart home, this can protect real power demand [160]. Similarly, purpose methods focus on using protocols based on cryptography for data aggregation [161], for fault tolerance [162] and do deal with the existence of untrusted aggregator [163]. Desired information about power consumption time series can be set secret (hidden) while preserving the utility of data [164]. Despite a general focus on technological challenges of big data on smart grids, a consensus exists about the challenges of how data analytics on smart meters data "enable involuntary and systematic insight into the daily patterns of the private life of individuals" [165].

3.5. Data ethics in the energy sector

Research on data ethics in the energy sector is scarce, even with the rise of ethical challenges brought by the spread of IoT and smart appliances. The details of the articles selected can be found on Table 7 of the Appendix.

Open investigations related to IoT rely on ethical aspects of security, privacy, and trust [166]. The ethics concerning big data analytics see the consequence of a hyper-networked society a power imbalance by societal actors, having a gradual decrease in individuals moral agency, and a strengthening of corporate agency [167]. Those concerns extend to the energy sector, Le Ray [32] argues that ethics should be on the basis for the development of smart grids, for reasons like the mandatory roll-out of smart meters appliances. Such mandatory regulation does not consider users views and power to decide over their private information. Lack of ethical guidance can generate low trust towards that technology and the institutions handlying the smart meters, thus challenging users' further possibilities to get involved with the technology that could result in energy-saving behaviour [32]. For instance, applying the Declaration of Human Rights (the individual's right to privacy [32]) should imply that people's home environment should not suffer outside interferences. This extends to all the smart city environments, where the list of individuals' privacy branches goes from surveillance (watching or recording users information), intrusion (invasive acts like notifications), to blackmail (disclosing users information) [168].

Furthermore, citizens' sharing private data with institutions and companies raise questions on data control, and who controls it. Users should have the right to decide who will have access to their data [32]. Customers controlling their data of the smart meters or being considered stakeholders in the energy sector could increase user awareness about efficient energy practices. However, amongst the problems of this narrative is that the smart meter's interfaces can be hard to comprehend for non-experts [32]. We need to advance the ethical regulations as fast as data analytics technology development, at least.

4. Discussion

In this section, we look back at the aims of the study and discuss how our findings help in addressing them. The main aim of this study is: to identify what the literature reports about surveillance capitalism practices and to correlate that with the discussions to do with trust in big data analysis, energy systems such as smart meters and high trust Scandinavian societies.

We can say that the monitoring of people's behaviour and the transgression of their privacy rights is identified as a threat to trustworthy cultures because their democratic processes and practices, central to their continuous development and welfare, are challenged by the misuse of data for inference and modification of users' behaviour and preferences, driven by corporate or governmental interests. Furthermore, the reported culture of trust in Scandinavia seems to guarantee companies the people's tolerance to the collection and processing of their data but may undermine users' conscious agency when it comes to the uses of their data. In this way, it is necessary to keep in mind that the current technological development that enabled and facilitated surveillance capitalism practices is developing faster than the legislations to regulate them. This means that people's activities inside their households are likely objects for increased data generation, analysis, and subsequent profit-making.

It requires a high level of trust from users to knowingly allow private companies or public government institutions to collect and analyse their data. In this article, we analysed and discussed how much trust the public could invest in energy companies that harvest and process people's data, given that we do not know yet where the rapid advancements of data processing technologies may lead [10 p. 509].

We were able to find an increased interest in developing smart technologies and techniques that collect and analyse detailed data about people's practices and smart platforms were identified to provide suitable profiling information. However, many papers are raising concerns about privacy issues, and most of them focus on developing protocols to protect users' privacy and data security. At this stage, it is not possible to discern from the existing literature whether the companies that are installing, maintaining, or supporting smart devices and have control of users' data, are selling such data to third parties, or using such data to generate products or services. We found no specific literature that examined the nature of consent people sign when they get connected to smart metre devices in Scandinavia. This could provide insights into the clauses in such agreements that protect people's privacy.

Access to primary domestic information through e.g. smart meters allows, from a technical point of view, not only the possibility to manage energy use (e.g. to decrease energy peak demand) but also to make inferences of users' patterns of behaviour. Although peak shaving and peak shifting can be beneficial for the grid and customers, if data processing practices are kept opaque for the customer, there is an increased likelihood that trust will be undermined out of fear of possible manipulation.

Furthermore, as shown by the articles reviewed that focus on data analytics techniques, third parties can use energy data and metadata to infer sensible and personal information whose value and danger may not be evident at present. This is a reason for concern because data collection is ubiquitous through advanced metering infrastructures and smart devices. Thus, data gathering technologies already invaded people's homes [55,68,131]. Surprisingly though, this is changing peoples' perception of what is private and their understanding of what constitutes their personal boundaries giving rise to security vulnerabilities. Scandinavian trust-based societies' progress is strongly driven by the implementation of innovations, some of which rely on big data. However, the moral values, public discussions, and collaborative tendency of individuals and institutions create an awareness of the vulnerabilities of dealing with networked digital devices. Hence, trust is balanced by rational distrust.

By analysing the methodological instruments used by the articles we identified a pattern where articles on the section "big data and trust" mostly use computational and modelling methods to deal with technicalities. In other side, e.g. Scandinavia trust use surveys and focus on people understanding of trust, correlation with behavioural characteristics.

Amongst our key findings, we encountered a growing trend in the development of privacy-preserving tools to protect the user's data, consequently increasing the trust in big data, and further developing smart systems technologies such as wearables and home appliances and collection for smart metre data. In Scandinavian countries, such innovations can potentially spread quickly because the trust relationships favour cooperation between citizens and the state, governments and public institutions, and public and private companies. This can favour the decarbonisation of the energy sector, but trust amongst those societies can decrease if, e.g. the purpose of smart metre data collection is not clarified to the citizens, since there is an apprehensiveness towards data-gathering technologies. It follows that surveillance capitalism indirectly challenges the cultural norms bringing new configurations to individuals, institutions, and relationships.

While privacy protection is a big challenge, due to the computational cost of handling and maintaining data quality while preserving users' anonymity, customers will need to have more control over who gets access and clarity about the purpose of the data collection. However, research focuses mostly on improving how we are processing data more effectively and not so much whether what is being processed could be harmful to people. The collection of personal behavioural information may path the way for energy data collection that potentially allows companies to regulate people's behaviour. Most of the research we identified on smart meters and big data focus on data collection and analysis but lesser on the consequences this may have for people's lives.

5. Conclusion and future work

In this article, we have proposed to carefully examine what the literature reports about surveillance capitalism practices, and how this shapes people's vulnerabilities and increases the need to trust those who are in power of processing data. We contextualised this by focusing on the energy sector and within this sector on smart meters. We examined questions of trust in the context of Scandinavian societies since they are reported to be high trust societies.

We chose this focus because it seemed particularly suitable for a systematic analysis of the literature, and we were not disappointed by what we were able to identify. Our analysis has allowed us to thematically group some well-known reports of (energy user) data processing and its effect on people's trust, but has also offered some interesting and unexpected observations (e.g. the vulnerability of technical solutions to protect people's privacy).

In the context of Scandinavian countries, the distribution system operators (DSOs) control users' data collection through smart meters. While data analytics of smart metre data is at an early stage of development, the main focus is often on optimisation strategies of the technology. We learned that Scandinavian citizens trust the intentions of the core institutions who collect data, but they are vigilant on actions taken. This indicates an existence of rational trust that allows innovation and development of innovative projects but also rational distrust that works as a form of control by citizens towards institutions who could profit from analytics of citizens data. Trust is showing to be fundamental to enhance cooperation between energy providers, distributors, and customers and thus comply with the aim of digitalisation of the energy sector by decreasing energy consumption.

In our literature review, we found no specific studies directly linking practices of surveillance capitalism in Scandinavia with energy data processing practices. However, we found evidence supporting a correlation between the Scandinavian culture of trust and ethical values like transparency, and social and environmental responsibility. The Scandinavian culture of trust is influenced by citizens sharing similar values, thus it can be argued that political decisions must reflect citizens interests to preserve this cultural characteristic. Controversies caused by distinct interests can harm mutual trust between citizens and institutions. For instance, if citizens feel they lost control over their private information or that data is used for a purpose that has not stated in the consent signed e.g. though smart meters, a position of rational distrust can be adopted. We conclude that the ongoing implementation of privacy-disrupting technologies in private homes, like smart meters, could endanger trust [32]. Given, the pivotal role of trust in Scandinavian's whole political and social infrastructures, it seems that there is a need for an ethical framework that can be applied and allows for more transparency and disclosure of data handling processes in the user contracts in the energy sector.

The literature review showed that data analytics algorithms can be used to infer people's behaviour, potentially revealing citizens' private information that is usually considered only accessible in the household. Eventually, organisations (or individuals on them) may develop interests in such data, and big-data technologies could provide them with the ability to get hold of privileged information and use it to make decisions over the smart energy systems. Without the extra inference power, such decisions would belong to or be influenced by individuals or other institutions. Therefore, besides possible violations of the human right of privacy preservation, without regulatory frameworks, there is a clear risk of expropriating the personal, bureaucratic or social agencies.

An accompanying problem is the increased tolerance for surveillance practices since the implementation of digital surveillance economies started. Framing societal problems as of technological nature put corporate interests at the centre and citizens are transformed in objects of datafication. Furthermore, companies and institutions may disregard the trust granted by users when data, or analysed data, is shared between monopolies, government, or other organisations. While using systematic review principles helped us to improve the quality of the literature review, it also a resource-intensive activity. Above all our hope was that it should help us to find a reasonable answer to our research question, but we are aware that the review here is not an end in itself. As mentioned at the beginning we made a decision to neglect some socio-cultural factors (migration, socio-economic factors) however, we are aware that they will have an impact on people's perception on how vulnerable they feel when data is collected from them.

We think that future studies could consider various kinds of appropriate 'ethical frameworks' to assess the case at hand. Currently, theory on data-ethics proliferate (e.g. Zwitter 2016 [167]), however broader frameworks that include assessments of social justice and citizens' autonomy and privacy protection could be relevant for future theory development [169,170]. For instance, basic liberal political theory, such as John Rawls' influential theory of justice (1971/1999) might provide outlines for such theory development [170]. This would include to abstain from deliberate ignorance of the consequences that are attached to consenting to data harvesting and equally to ignoring the consequences when data processing algorithms are profit driven. Needless to say, it goes beyond this article's scope to enter this issue further.

Co-authorship

Co-authorship followed the guidelines of the Vancouver agreement.

Declaration of Competing Interest

The authors declare no conflict of interests.

Acknowledgements

This work was supported by ENSYSTRA (this project has received funding from the European Union Horizon 2020 research and innovation programme under the Marie Sklodowska-Curie grant agreement No 765515).

Appendix A

Tables 3–7.

Table 3
Themes and methodologies under of the topic "Surveillance capitalism".

Theme	Reference	No. of papers	Methods used

Control	[14]; [36]; [46–53].	10	[14] Theoretical argumentation and document analysis;
			[36] Theoretical review;
			[46] Discussion group, interviews and grounded theory;
			[47] Conceptual framework;
			[48] Case study;
			[49] Theoretical review;
			[50] Case study;
			[51] Theoretical argumentation;
			[52] Theoretical analysis;
			[53] Case study, comparative analysis.

Privacy	[54]; [55]; [56].	3	[54] Theoretical argumentation, case study; [55] Cross-Cultural focus group; [56] Network analysis.
Cultural Impact	[57, 58].	2	[57] Case study; [58] Theoretical argumentation.

Business Models	[59–62].	4	[59] Empirical research (literature review, conceptual maps);
			[60] Theoretical analysis;
			[61] Theoretical analysis;
			[62] Document analysis.

Market Sectors	[13]; [63–66].	5	[13] Theoretical argumentation; [63] Theoretical argumentation and case study; [64] Literature review; [65] Theoretical argumentation and case study; [66] Theoretical argumentation and case study.

Smart Technologies	[67–69].	3	[67] Theoretical argumentation;
			[68] Empirical research;
			[69] Theoretical argumentation.

GDPR	[70–72].	3	[70] Case study;
			[71] Theoretical argumentation;
			[72] Case study.

		30	

Table 4
Themes and methodological analysis of the topic “trust culture in Scandinavia”.

Themes	References	No. of papers	Methods used
Economic development	[73, 74].	2	[73] Theoretical argumentation; [74] Case study and interviews.
Control	[75, 76].	2	[75] Case study, cross-country comparision and qualitative analysis; [76] Case study, empirical analysis.

Institutional trust	[77–84].	8	[77] Qualitative textual analysis;
			[78] Empirical analysis;
			[79] Case study;
			[80] Empirical analysis;
			[81] Theoretical argumentation;
			[82] Theoretical argumentation;
			[83] Interview, cross-country comparison;
			[84] Theoretical argumentation, case study.

Interpersonal trust (social trust)	[28, 85–88].	5	[28] Survey;
			[85] Survey;
			[86] Survey;
			[87] Survey;
			[88] Interviews.

Ethics	[89]	1	[89] Theoretical argumentation, case study.
Social and environmental responsibility	[90–94].	5	[90] Theoretical argumentation, case study; [91] Theoretical argumentation, case study; [92] Survey; [93] Cross-country comparison, case study; [94] Survey.

Digital trust	[95–97].	3	[95] Survey, cross-country comparison;
			[96] Theoretical argumentation;
			[97] Survey, cross-country comparison.

Total		26	

Table 5
Themes analysis of the “big data” and “trust” papers reviewed.

Theme	Author/ Papers	No. of papers	Methods

Datafication, Dataveillance/Surveillance	[98–101].	4	[98] Survey;
			[99] Theoretic argumentation;
			[100] Theretical framework, case study;
			[101] Theoretical argumentation.

Privacy and security	[102–104].	3	[102] Review;
			[103] Review;
			[104] Review.

Ethics, philosophy and ideologies	[105–111].	7	[105] Focus group;
			[106] Review;
			[107] Theoretical argumentation;
			[108] Theoretical Argumentation;
			[109] Theoretical argumentation;
			[110] Theoretical argumentation;
			[111] Theoretical argumentation.

Behaviour	[112–117].	6	[112] Grounded theory, interviews, case study;
			[113] Survey;
			[114] Systematic literature review;
			[115] Survey;
			[116] Interviews;
			[117] Survey.

Governance	[118–121].	4	[118] Systematic literature review, case study; [119] Theoretical argumentation; [120] Mathematical modelling and software implementation; [121] Interviews.

(continued on next page)

Table 5 (*continued*)

Theme	Author/ Papers	No. of papers	Methods

GDPR	[122–126].	5	[122] Cross-contry comparisson;
			[123] Computational modelling;
			[124] Tool validation;
			[125] Review;
			[126] Ethnography.

Smart Technologies	[127–139].	13	[127] Empirical analysis, interviews;
			[128] Theoretical argumentation;
			[129] Empirical analysis, tool development;
			[130] Theoretical argumentation;
			[131] Empirical analysis;
			[132] Empirical analysis, semi-structured interviews;
			[133] Survey and case study;
			[134] Review, application development;
			[135] Review;
			[136] Mathematical modelling;
			[137] Technique development, optimization;
			[138] Mathematic modelling, computational modelling;
			[139] Machine learning.

Total		42	

Table 6
Themes analysed and research methods explored under the topic “Big Data” AND “Smart Meters”.

Theme	Papers	No. of papers	Methodology

Energy data analytics	[140–147].	8	[140] Mix–methods (book);
			[141] Empirical analysis;
			[142] Review;
			[143] Review;
			[144] Empirical analysis;
			[145] Computational modelling;
			[146] Empirical analysis, computational modelling;
			[147] Theoretical argumentation, computational modelling.

Data-based applications	[148–153].	6	[148] Modelling, empirical analysis;
			[150] Review, theoretical argumentation;
			[149] Empirical analysis;
			[151] Empirical analysis;
			[152] Empirical analysis;
			[153] Case study, empirical analysis.

Market research	[154–156].	3	[154] Review; [155] Literature review and experts interview; [156] Computational modelling.
Security	[157–159].	3	[157] Empirical analysis, computation modelling; [158] Computational modelling, empirical analysis; [159] Computational modelling.

Privacy	[160–165].	6	[160] Computational modelling;
			[161] Computational modelling;
			[162] Computational modelling;
			[163] Computational modelling;
			[164] Mathematical modelling;
			[165] Review.

Total		26	

Table 7
Themes analysed and research methods explored under the topic “Data Ethics” AND “Energy Sector”.

Theme	Papers	No. of papers	Methodology
Regulations	[32,166].	2	[32] Theoretical argumentation; [166] Review.
Foundations	[167,168].	2	[167] Theoretical argumentation; [168] Theoretical argumentation.
Total		4	

References

[1] Jin D, Ocone R, Jiao K, Xuan J. Energy and AI. Energy AI 2020;1:100002. doi:10.1016/j.egyai.2020.100002.

[2] Zhou S, Brown MA. Smart meter deployment in Europe : a comparative case study on the impacts of national policy schemes. J Clean Prod 2017;144:22–32. doi:10.1016/j.jclepro.2016.12.031.

[3] Zwitter A. Big Data ethics. Big Data Soc 2014;1(2) p. 205395171455925. doi:10.1177/2053951714559253.

[4] Rose G. Visual Methodologies: an Introduction to Researching with Visual Materials. 2rd ed.. Sage Publ Ltd 2007;49(4):449–51. doi:10.1111/j.1755-618x.2012.01310.x.

[5] Loveless A, Williamson B. Shaping society, technology. In: Learning Identities in a Digital Age: Rethinking Creativity, Education and Technology; 2013. p. 7–30. Routlege, Ed. London.

[6] Politou E, Alepis E, Patsakis C. Forgetting personal data and revoking consent under the GDPR: challenges and Proposed Solutions. J Cybersecurity 2018(April):1–20. doi:10.1093/CYBSEC/TYY001.

[7] Flyverbom M, Deibert R, Matten D. The governance of digital technology, big data, and the internet: new roles and responsibilities for business. Bus Soc; 2017. doi:101177/0007650317727540.

[8] Bruun MH, Andersen AO, Mannov A. Infrastructures of trust and distrust: the politics and ethics of emerging cryptographic technologies. Anthropol Today 2020;36(2):13–17. doi:10.1111/1467-8322.12562.

[9] Zuboff S. The age of surveillance capitalism: the fight for a human future at the new frontier of power. Barack Obama's Book of 2019; 2019.

[10] S. Sagiroglu and D. Sinanc, "Big Data : a Review," pp. 42–47, 2013.

[11] J. Cobbe, "Algorithmic surveillance," pp. 1–30, 2018.

[12] Ward K. Social networks, the 2016 US presidential election, and Kantian ethics: applying the categorical imperative to Cambridge analytica's behavioral microtargeting. J Media Ethics Explor Quest Media Moral 2018;33(3):133–48. doi:10.1080/23736992.2018.1477047.

[13] Barassi V. Datafied citizens in the age of coerced digital participation. Sociol Res Online 2019;24(3):414–29. doi:10.1177/1360780419857734.

[14] Zuboff S. Big other: surveillance capitalism and the prospects of an information civilization. J Inf Technol 2015;30(1):75–89. doi:10.1057/jit.2015.5.

[15] Simon J. The onlife manifesto: being human in a hyperconnected era; 2015.

[16] Dencik L, Hintz A, Cable J. Towards data justice? The ambiguity of anti-surveillance resistance in political activism. Big Data Soc 2016;3(2):1–12. doi:10.1177/2053951716679678.

[17] Lupton D, Williamson B. The datafied child: the dataveillance of children and implications for their rights. New Media Soc 2017;19(5):780–94. doi:10.1177/1461444816686328.

[18] A.S.-K.D.B. Kristensenn, Redistribution of Medical Responsibility in the Network of the Hyper-connected Self. 2019.

[19] Mckenna E, Richardson I, Thomson M. Smart meter data : balancing consumer privacy concerns with legitimate applications. Energy Policy 2012;41:807–14. doi:10.1016/j.enpol.2011.11.049.

[20] Rubinstein IS. Big data: the end of privacy or a new beginning? Int Data Priv Law 2012;3(2):74–87. doi:10.1093/idpl/ips036.

[21] Gefen D. E-commerce: The role of familiarity and trust. Omega (Westport) 2000;28(6):725–37. doi:10.1016/S0305-0483(00)00021-9.

[22] C.S. the dangers of openly sharing and covertly collecting data Shareveillance: the dangers of openly sharing and covertly collecting data U of M P Birchall. Univ Minnesota Press; 2017.

[23] H. Felzmann, E.F. Villaronga, C. Lutz, and A. Tamo, "Transparency you can trust : transparency requirements for artificial intelligence between legal norms and contextual concerns," no. June, pp. 1–14, 2019, doi: 10.1177/2053951719860542.

[24] Terzi DS, Demirezen U, Sagiroglu S. Evaluations of big data processing. Serv Trans Big Data 2016;3(1):44–53.

[25] Bellaby P, Eames M, Flynn R. The role of 'trust' in the transition to sustainable energy. Energy Policy 2010;38(6):2613–14. doi:10.1016/j.enpol.2009.03.066.

[26] Ceglarz A, Beneking A, Ellenbeck S, Battaglini A. Understanding the role of trust in power line development projects: evidence from two case studies in Norway. Energy Policy 2017;110(March):570–80. doi:10.1016/j.enpol.2017.08.051.

[27] Liu L, Bouman T, Perlaviciute G, Steg L. Effects of trust and public participation on acceptability of renewable energy projects in the Netherlands and China. Energy Res Soc Sci 2019;53(March):137–44. doi:10.1016/j.erss.2019.03.006.

[28] Beilmann M, Lilleoja L. Social trust and value similarity: the relationship between social trust and human values in Europe. Stud Transit States Soc 2015;7(2):19–30.

[29] Ballo IF. Imagining energy futures: sociotechnical imaginaries of the future Smart Grid in Norway. Energy Res Soc Sci 2015;9:9–20. doi:10.1016/j.erss.2015.08.015.

[30] Naus J, Van Vliet BJM, Hendriksen A. Households as change agents in a Dutch smart energy transition: on power, privacy and participation. Energy Res Soc Sci 2015;9:125–36. doi:10.1016/j.erss.2015.08.025.

[31] Bertoldo R, Poumadère M, Rodrigues LC. When meters start to talk: the public's encounter with smart meters in France. Energy Res Soc Sci 2015;9:146–56. doi:10.1016/j.erss.2015.08.014.

[32] Le Ray G, Pinson P. The ethical smart grid: enabling a fruitful and long-lasting relationship between utilities and customers. Energy Policy 2020;140(January):111258. doi:10.1016/j.enpol.2020.111258.

[33] Huang Y, Grahn E, Wallnerströn CJ, Jaakonantti L, Johansson T. Smart meters in Sweden – lessons learned and new regulations. 3rd AIEE Symp Curr Futur Challenges to Energy Secur 2018(December):12.

[34] J. De Godoy, "Annotated bibliography: actor behavior and interactions in the context of sustainable energy transitions," 2020.

[35] Love J, Cooper ACG. From social and technical to socio-technical: designing integrated research on domestic energy use. Indoor Built Environ 2015;24(7):986–98. doi:10.1177/1420326X15601722.

[36] Galič M, Timan T, Koops BJ. Bentham, Deleuze and beyond: an overview of surveillance theories from the panopticon to participation. Philos Technol 2017;30(1):9–37. doi:10.1007/s13347-016-0219-1.

[37] Stephenson J, et al. Energy research & social science the energy cultures framework : exploring the role of norms, practices and material culture in shaping energy behaviour in New Zealand. Energy Res Soc Sci 2015;7:117–23. doi:10.1016/j.erss.2015.03.005.

[38] Stephenson J, Barton B, Carrington G, Gnoth D, Lawson R, Thorsnes P. Energy cultures : a framework for understanding energy behaviours. Energy Policy 2010;38(10):6120–9. doi:10.1016/j.enpol.2010.05.069.

[39] Ginieis M, Sánchez-Rebull MV, Campa-Planas F. The academic journal literature on air transport: analysis using systematic literature review methodology. J Air Transp Manag 2012;19(1):31–5. doi:10.1016/j.jairtraman.2011.12.005.

[40] Pittaway L, Robertson M, Munir K, Denyer D, Neely A. Networking and innovation: a systematic review of the evidence. Int J Manag Rev 2004;5–6(3–4):137–68. doi:10.1111/j.1460-8545.2004.00101.x.

[41] Castleberry A, Nolen A. Thematic analysis of qualitative research data: is it as easy as it sounds? Curr Pharm Teach Learn 2018;10(6):807–15. doi:10.1016/j.cptl.2018.03.019.

[42] Braun V, Clarke V. Qualitative research in psychology using thematic analysis in psychology using thematic analysis in psychology. Qual Res Psychol 2006;3(2):77–101.

[43] Keele S. Performing systematic literature reviews in software engineering. Tech report, Ver 23 EBSE Tech Report EBSE 2007;2006(5):65 Vol.. doi:10.1145/1134285.1134500.

[44] Braun V, Clarke V. Reflecting on reflexive thematic analysis. Qual Res Sport Exerc Heal 2019;11(4):589–97. doi:10.1080/2159676X.2019.1628806.

[45] Mannov A, Andersen AOberborbeck, Godoy J. The age of surveillance capitalism. the fight for a human future: at the new frontier of power. Tecnoscienza Ital J Sci Technol Stud 2020;11(1):109–13.

[46] Moro A, Rinaldini M, Staccioli J, Virgillito ME. Control in the era of surveillance capitalism: an empirical investigation of Italian Industry 4.0 factories. J Ind Bus Econ 2019;46(3):347–60. doi:10.1007/s40812-019-00120-2.

[47] Kwet M. Digital colonialism: US empire and the new imperialism in the Global South. Race Cl 2019;60(4):3–26. doi:10.1177/0306396818823172.

[48] Jain S, Gabor D. The rise of digital financialisation: the case of India. New Polit Econ 2020;25(5):813–28. doi:10.1080/13563467.2019.1708879.

[49] Onsrud H, Campbell J. Being human in an algorithmically controlled world. Int J Humanit Arts Comput 2020;14(1):235–52.

[50] Firmino RJ, de V Cardoso B, Evangelista R. Hyperconnectivity and (Im)mobility: uber and surveillance capitalism by the Global South. Surveill Soc 2019;17(1–2):205–12. doi:10.24908/ss.v17i1/2.12915.

[51] Maavak M. Bubble to panopticon: dark undercurrents of the big data torrent. Kybernetes 2019;49(3):1046–60. doi:10.1108/K-06-2019-0403.

[52] Charitsis V, Zwick D, Bradshaw A. Creating worlds that create audiences: theorising personal data markets in the age of communicative capitalism. TripleC 2018;16(2):820–34. doi:10.31269/triplec.v16i2.1041.

[53] Kumar P. Corporate privacy policy changes during PRISM and the rise of surveillance capitalism. Media Commun 2017;5(1):63–75. doi:10.17645/mac.v5i1.813.

[54] Slaughter RA. The IT revolution reassessed part two: case studies and implications. Futures 2018;98(November 2017):19–31. doi:10.1016/j.futures.2017.12.007.

[55] Pridmore J, et al. Intelligent personal assistants and the intercultural negotiations of dataveillance in platformed households. Surveill Soc 2019;17(1–2):125–31. doi:10.24908/ss.v17i1/2.12936.

[56] Libert T, Binns R. Good news for people who love bad news: centralization, Privacy, and transparency on us news sites. In: WebSci 2019 - Proc. 11th ACM Conf. Web Sci; 2019. p. 155–64. doi:10.1145/3292522.3326019.

[57] Partin WC. Watch me pay: twitch and the cultural economy of surveillance. Surveill Soc 2019;17(1/2):153–60. doi:10.24908/ss.v17i1/2.13021.

[58] J. Cinnamon, "Social injustice in surveillance capitalism," vol. 15, no. 5, pp. 609–25, 2017.

[59] Clarke R. Risks inherent in the digital surveillance economy: a research agenda. J Inf Technol 2019;34(1):59–80. doi:10.1177/0268396218815559.

[60] Landwehr M, Borning A, Wulf V. The high cost of free services: problems with surveillance capitalism and possible alternatives for IT infrastructure. ACM Int Conf Proceeding Ser 2019. doi:10.1145/3338103.3338106.

[61] Malmgren E. Resisting 'big other': what will it take to defeat surveillance capitalism? New Labor Forum 2019;28(3):42–50. doi:10.1177/1095796019864097.

[62] Rider K, Murakami Wood D. Condemned to connection? Network communitarianism in Mark Zuckerberg's 'Facebook manifesto. New Media Soc 2019;21(3):639–54. doi:10.1177/1461444818804772.

[63] Holloway D. Surveillance capitalism and children's data: the Internet of toys and things for children. Media Int Aust 2019;170(1):27–36. doi:10.1177/1329878X19828205.

[64] Mascheroni G. Datafied childhoods: contextualising datafication in everyday life. Curr Sociol 2018:1–16. doi:10.1177/0011392118807534.

[65] Gidaris C. Surveillance capitalism, datafication, and unwaged labour: the rise of wearable fitness devices and interactive life insurance. Surveill Soc 2019;17(1–2):132–8. doi:10.24908/ss.v17i1/2.12913.

[66] Rosamond E. To sort, to match and to share: addressivity in online dating platforms. J Aesthet Cult 2018;10(3):32–42. doi:10.1080/20004214.2017.1400864.

[67] León LFA, Rosen J. Technology as Ideology in Urban Governance. Ann Am Assoc Geogr 2020;110(2):497–506. doi:10.1080/24694452.2019.1660139.

[68] Pridmore J, Mols A. Personal choices and situated data: privacy negotiations and the acceptance of household Intelligent Personal Assistants. Big Data Soc 2020;7(1). doi:10.1177/2053951719891748.

[69] Lacey C, Caudwell C. Cuteness as a ‘dark pattern’ in home robots. ACM/IEEE Int Conf Human-Robot Interact 2019:374–81 vol. 2019-March. doi:10.1109/HRI.2019.8673274.

[70] Aho B, Duffield R. Beyond surveillance capitalism: privacy, regulation and big data in Europe and China. Econ Soc 2020;49(2):187–212. doi:10.1080/03085147.2019.1690275.

[71] Andrew J, Baker M. The general data protection regulation in the age of surveillance capitalism. J Bus Ethics 2019(0123456789). doi:10.1007/s10551-019-04239-z.

[72] Kuntsman A, Miyake E, Martin S. *Re*-thinking digital health: data, appisation and the (im)possibility of ‘opting out. Digit Heal 2019;5:1–16. doi:10.1177/2055207619880671.

[73] Svendsen GLH, Svendsen GT. How did trade norms evolve in Scandinavia? Long-distance trade and social trust in the Viking age. Econ Syst 2016;40(2):198–205. doi:10.1016/j.ecosys.2016.03.001.

[74] Nicolajsen HW, Scupola A. Investigating issues and challenges for customer involvement in business services innovation. J Bus Ind Mark 2011;26(5):368–76. doi:10.1108/08858621111144424.

[75] Listhaug O. Oil wealth dissatisfaction and political trust in Norway: a resource curse? West Eur Polit 2005;28(4):834–51. doi:10.1080/01402380500216955.

[76] Lueg R. How do Controls and Trust INteract? The case of failed alliance negotiations in the financial services industry. Int J Bus Res 2014;14(1):127–48.

[77] H. Askeland, G. Espedal, B.Jelstad Løvaas, and S. Sirris, *Understanding Values Work: Institutional Perspective in Organizations and Leadership*. palgrave macmillan, 2020.

[78] Torpe L. Corporatism and Social Trust: bringing Voluntary Organizations ‘Back In. J Civ Soc 2014;10(2):204–18. doi:10.1080/17448689.2014.922748.

[79] Ghazinejad M, Hussein BA, Zidane YJT. Impact of trust, commitment, and openness on research project performance: case study in a research institute. Soc Sci 2018;7(2). doi:10.3390/socsci7020022.

[80] Marozzi M. Measuring trust in European public institutions. Soc Indic Res 2015;123(3):879–95. doi:10.1007/s11205-014-0765-9.

[81] Rothstein B, Stolle D. Introduction: social capital in Scandinavia. Scan Polit Stud 2003;26(1):1–26. doi:10.1111/1467-9477.t01-1-00077.

[82] Selle P, Wollebæk D. The complex relationship between civil society and trust. Ital Sociol Rev 2015;5(3):273–91. doi:10.13136/isr.v5i3.110.

[83] Paik Y, Warner-Søderholm G, Huse M. In search of an institutional framework for anticorruption: lessons from Scandinavia. Thunderbird Int Bus Rev 2019;61(2):105–18. doi:10.1002/tie.22028.

[84] Martin CJ. Cooperation for innovation: a solidaristic approach to economic reform. Juncture 2014;21(1):48–52. doi:10.1111/j.2050-5876.2014.00779.x.

[85] Albanese G, de Blasio G. Who trusts others more? A cross-European study. Empirica 2014;41(4):803–20. doi:10.1007/s10663-013-9238-7.

[86] Sjöberg L, Herber MW. Too much trust in (social) trust? The importance of epistemic concerns and perceived antagonism. Int J Glob Environ Issues 2008;8(1–2):30–44. doi:10.1504/IJGENVI.2008.017258.

[87] Wollebæk D, Lundåsen SW, Trägårdh L. Three forms of interpersonal trust: evidence from Swedish municipalities. Scan Polit Stud 2012;35(4):319–46. doi:10.1111/j.1467-9477.2012.00291.x.

[88] Gulbrandsen T. Norway : trust among elites in a corporatist democracy. Comp Sociol 2005;4(1):112–35.

[89] Rendtorff JD. The honest businessperson: cosmopolitan theory and cultural praxis (the example of Denmark and Scandinavia. Ethical Econ 2019;56:41–53. doi:10.1007/978-3-030-04351-3_4.

[90] Stenseke M. Local participation in cultural landscape maintenance: lessons from Sweden. Land Use Policy 2009;26(2):214–23. doi:10.1016/j.landusepol.2008.01.005.

[91] Strand R. Corporate responsibility in scandinavian supply chains. J Bus Ethics 2009;85(SUPPL. 1):179–85. doi:10.1007/s10551-008-9937-3.

[92] Viklund M. Energy policy options-from the perspective of public attitudes and risk perceptions. Energy Policy 2004;32(10):1159–71. doi:10.1016/S0301-4215(03)00079-X.

[93] Dawson J, Darst R. Meeting the challenge of permanent nuclear waste disposal in an expanding Europe: transparency, trust and democracy. Env Polit 2006;15(4):610–27. doi:10.1080/09644010600785226.

[94] Sjöberg L. Local acceptance of a high-level nuclear waste repository. Risk Anal 2004;24(3):737–49. doi:10.1111/j.0272-4332.2004.00472.x.

[95] Kivijärvi M, Laukkanen T, Cruz P. Consumer trust in electronic service consumption: a cross-cultural comparison between Finland and Portugal. J Euromarketing 2007;16(3):51–65. doi:10.1300/J037v16n03_05.

[96] Andreassen OA. eHealth provides a novel opportunity to exploit the advantages of the Nordic countries in psychiatric genetic research, building on the public health care system, biobanks, and registries. Am J Med Genet Part B Neuropsychiatr Genet 2018;177(7):625–9. doi:10.1002/ajmg.b.32561.

[97] Evjemo B, Castejón-Martínez H, Akselsen S. Trust trumps concern: findings from a seven-country study on consumer consent to ‘digital native’ vs. ‘digital immigrant’ service providers. Behav Inf Technol 2019;38(5):503–18. doi:10.1080/0144929X.2018.1541254.

[98] Leckner S. Sceptics and supporters of corporate use of behavioural data: attitudes towards informational privacy and Internet surveillance in Sweden, Northern Lights. Film & Media Studies Yearbook 2018;16:113–32. doi:10.1386/nl.16.113.

[99] van Dijck J. Datafication, dataism and dataveillance: big data between scientific paradigm and ideology. Surveill Soc 2014;12(2):197–208. doi:10.24908/ss.v12i2.4776.

[100] Rajamäki J, Simola J. How to apply privacy by design in OSINT and big data analytics?. In: ECCWS 2019 Proc. 18th Eur. Conf. Cyber Warf. Secur; 2019. p. 364–71.

[101] G.L. Gilbert, “Communicable disease surveillance ethics in the age of big data and new technology,” pp. 173–87, 2019.

[102] Keller SA, Shipp S, Schroeder A. Does big data change the privacy landscape? A review of the Issues. Annu Rev Statistics Appl 2016(March):1–20. doi:10.1146/annurev-statistics-041715-033453.

[103] Li S, Gao J. Security and privacy for big data. Springer International Publishing Switzerland; 2016.

[104] Demchenko Y, Ngo C, De Laat C, Membrey P, Gordijenko Daniil. Big security for big data : addressing security challenges for the big data infrastructure. In: In Workshop on Secure Data Management; 2013. p. 76–94.

[105] Varley-winter O, Shah H, Society RS, Street E, Ecy L, Varley-winter O. The opportunities and ethics of big data: practical priorities for a national Council of Data Ethics Author for correspondence. Philos Trans A 2016.

[106] Penneck S. Confidentiality in an era of big data: an official statistics perspective. Stat J IAOS 2019;35:353–8. doi:10.3233/SJI-190501.

[107] Gorur R. Afterword: embracing numbers? Int Stud Sociol Educ 2020;29(1–2):187–97. doi:10.1080/09620214.2020.1720518.

[108] Lehikoinen V, Koistinen J. In big data we trust. Interactions 2014:38–41.

[109] Baru C. Data in the 21 st Century. Springer Int Publ 2018;2:3–17 doi: doi.org/. doi:10.1007/978-3-319-70942-0_1.

[110] First D. Will big data algorithms dismantle the foundations of liberalism ? AI Soc 2018;33(4):545–56. doi:10.1007/s00146-017-0733-4.

[111] Woolley JP. Trust and justice in big data analytics : bringing the philosophical literature on trust to bear on the ethics of. Philos Technol 2019;32(1) doi: http://dx.doi.org.manchester.idm.oclc.org/Abstract:. doi:10.1007/s13347-017-0288-9.

[112] I.B. Pugna, A. Dut, and O. Georgiana, “Corporate attitudes towards big data and its impact on performance management : a qualitative study,” 2019, doi: 10.3390/su11030684.

[113] Wang Z, Yu Q. Privacy trust crisis of personal data in China in the era of big data : the survey and countermeasures. Comput Law Secur Rev Int J Technol Law Pract 2015;31(6):782–92. doi:10.1016/j.clsr.2015.08.006.

[114] S.S. Muhammad, B.L. Dey, and V. Weerakkody, “Analysis of factors that influence customers ’ willingness to leave big data digital footprints on social media : a systematic review of literature,” no. 2018, pp. 559–76, 2020, doi: 10.1007/s10796-017-9802-y.

[115] Chang Y, Wong SF, Libaque-saenz CF, Lee H. The role of privacy policy on consumers’ perceived privacy. Gov Inf Q 2018;35(3):445–59. doi:10.1016/j.giq.2018.04.002.

[116] Broekstra R, Aris-meijer J, Maeckelberghe E, Stolk R, Otten S. Trust in centralized large-scale data repository : a qualitative analysis. Journal of Empirical Research on Human Research Ethics 2020. doi:10.1177/1556264619888365.

[117] Xie W, Karan K. Consumers ’ privacy concern and privacy protection on social network sites in the era of big data : empirical evidence from college students consumers ’ privacy concern and privacy protection on social network sites in the era of big data : empirical evid. J Interact Advert 2019;19(3):187–201. doi:10.1080/15252019.2019.1651681.

[118] Brous P, Janssen M, Schraven D, Spiegeler J, Duzgun BC. Factors influencing adoption of IoT for data-driven decision making in asset management organizations. IoTBDS 2017:70–9. doi:10.5220/0006296300700079.

[119] G. Rieder and J. Simon, “Datatrust : or, the political quest for numerical evidence and the epistemologies of Big Data,” no. June, pp. 1–6, 2016, doi: 10.1177/2053951716649398.

[120] K. Theuermann, “Trustworthy privacy-preserving service compositions,” 2019, pp. 10–17, doi: 10.1109/TrustCom/BigDataSE.2019.00012.

[121] Praditya D. Assessment of factors influencing information sharing arrangements using the best-worst method, In Conference on e-Business, e-Services and e-Society 2017;21:94–106. doi:10.1007/978-3-319-68557-1.

[122] Custers B, Dechesne F, Sears AM, Tani T, Van Der Hof S. A comparison of data protection legislation and policies across the EU. Comput Law Secur Rev Int J Technol Law Pract 2018;34(2):234–43. doi:10.1016/j.clsr.2017.09.001.

[123] R. Ladjel, N. Anciaux, P. Pucheral, and G. Scerri, “Trustworthy distributed computations on personal data using trusted execution environments,” pp. 381–8, 2019, doi: 10.1109/TrustCom/BigDataSE.2019.00058.

[124] S. Fischer-hübner et al., “Transparency, privacy and trust – technology for tracking and controlling my data disclosures : does this work ? To cite this version : HAL Id : hal-01438345 transparency, privacy and trust – technology for tracking and controlling my data disclosures:,” 2017.

[125] B. Hoanca, C.M. Marinchak, and E. Forrest, “Ethical implications of the general data protection directive for virtual personal marketing assistants,” pp. 4073–80, 2018.

[126] Ruppert E, Grommé F, Ustek-Spilda F, Cakici B. Citizen data and trust in official statistics. Econ Stat 2018;2018(505–506):179–93. doi:10.24187/ecostat.2018.505d1971.

[127] McMillan D. Connecting citizens: designing for data collection and dissemination in the smart city. Lect Notes Comput Sci (including Subser Lect Notes Artif Intell Lect Notes Bioinformatics) 2017;10673:119–31 LNCS. doi:10.1007/978-3-319-70284-1_10.

[128] A. Cavoukian and M. Chibba, “Cognitive cities, big data and citizen participation : the essentials of privacy and security Á security Á big data Á,” pp. 61–82, 2016, doi: 10.1007/978-3-319-33798-2.

[129] Matheus R, Janssen M, Maheshwari D. Data science empowering the public: data-driven dashboards for transparent and accountable decision-making in smart cities. Gov Inf Q 2020;37(3):101284. doi:10.1016/j.giq.2018.01.006.

[130] Ranchordás S. Nudging citizens through technology in smart cities. Int Rev Law, Comput Technol 2020;34(3):254–76. doi:10.1080/13600869.2019.1590928.

[131] Furey E, Blue J. Can i trust her? Intelligent personal assistants and GDPR. In: 2019 Int. Symp. Networks, Comput. Commun. ISNCC; 2019. p. 2019. doi:10.1109/ISNCC.2019.8909098.

[132] Jakku E, et al. 'If they don't tell us what they do with it, why would we trust them?' Trust, transparency and benefit-sharing in Smart Farming. NJAS - Wageningen J Life Sci 2019;90–91(December 2018):100285. doi:10.1016/j.njas.2018.11.002.

[133] Beal CD, Flynn J. Toward the digital water age: survey and case studies of Australian water utility smart-metering programs. Util Policy 2015;32:29–37. doi:10.1016/j.jup.2014.12.006.

[134] Li S. Application of blockchain technology in smart city infrastructure. In: Proc. - 2018 IEEE Int. Conf. Smart Internet Things, SmartIoT 2018; 2018. p. 276–82. doi:10.1109/SmartIoT.2018.00056.

[135] Chin J, Callaghan V, Ben Allouch S. The internet-of-things: reflections on the past, present and future from a user-centered and smart environment perspective. J Ambient Intell Smart Environ 2019;11(1):45–69. doi:10.3233/AIS-180506.

[136] Anjum A, et al. Privacy preserving data by conceptualizing smart cities using MIDR-Angelization. Sustain Cities Soc 2018;40(January):326–34. doi:10.1016/j.scs.2018.04.014.

[137] Babar M, et al. A secured data management scheme for smart societies in industrial internet of things environment. IEEE Access 2018;6:43088–99. doi:10.1109/ACCESS.2018.2861421.

[138] Chifor BC, Bica I, Patriciu VV. Sensing service architecture for smart cities using social network platforms. Soft Comput 2017;21(16):4513–22. doi:10.1007/s00500-016-2053-x.

[139] Obert J, Chavez A, Johnson J. Behavioral based trust metrics and the smart grid. In: Proc. - 17th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. 12th IEEE Int. Conf. Big Data Sci. Eng. Trust. 2018; 2018. p. 1490–3. doi:10.1109/TrustCom/BigDataSE.2018.00209.

[140] Wang C, Wang Y, Chen W. Smart Meter Data Analytics 2020;1(1).

[141] Puangpontip S, Hewett R. Predicting customer behaviors on energy consumption: why past usage data are not enough?. In: Proc. - 2018 IEEE Int. Conf. Big data, big data 2018; 2019. p. 4577–81. doi:10.1109/BigData.2018.8622034.

[142] Wang Y, Chen Q, Hong T, Kang C. Review of smart meter data analytics: applications, methodologies, and challenges. IEEE Trans Smart Grid 2019;10(3):3125–48. doi:10.1109/TSG.2018.2818167.

[143] Bhawna ADhupia, Usha Rani, Alameen. Advances in intelligent systems and computing 1054 emerging research in data engineering systems and computer communications, 1054. Springer Singapore; 2019.

[144] Mohammad R. AMI smart meter big data analytics for time series of electricity consumption. In: Proc. - 17th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. 12th IEEE Int. Conf. Big Data Sci. Eng. Trust. 2018; 2018. p. 1771–6. doi:10.1109/TrustCom/BigDataSE.2018.00267.

[145] Hong T, Macumber D, Li H, Fleming K, Wang Z. Generation and representation of synthetic smart meter data. Build Simul 2020;1. doi:10.1007/s12273-020-0661-y.

[146] Ushakova A, Mikhaylov SJankin. Big data to the rescue? Challenges in analysing granular household electricity consumption in the United Kingdom. Energy Res Soc Sci 2020;64(February 2019):101428. doi:10.1016/j.erss.2020.101428.

[147] Dollah R, Aris H. A big data analytics model for household electricity consumption tracking and monitoring. In: 2018 IEEE Conf. Big Data Anal. ICBDA 2018; 2019. p. 44–9. doi:10.1109/ICBDAA.2018.8629769.

[148] Singh S, Yassine A, Benlamri R. Consumer segmentation: improving energy demand management through households socio-analytics. In: Proc. - IEEE 17th Int. Conf. Dependable, Auton. Secur. Comput. IEEE 17th Int. Conf. Pervasive Intell. Comput. IEEE 5th Int. Conf. Cloud Big Data Comput. 4th Cyber Sci; 2019. p. 1038–45. doi:10.1109/DASC/PiCom/CBDCom/CyberSciTech.2019.00187.

[149] Sial A, Singh A, Mahanti A. Detecting anomalous energy consumption using contextual analysis of smart meter data. Wirel Networks 2019;8. doi:10.1007/s11276-019-02074-8.

[150] Webborn E, Elam S, McKenna E, Oreszczyn T. Utilising smart meter data for research and innovation in the UK. Eceee Summer Study Proc 2019;2019-June:1387–96.

[151] Ullah A, et al. Deep learning assisted buildings energy consumption profiling using smart meter data. Sensors (Switzerland) 2020;20(3):1–15. doi:10.3390/s20030873.

[152] Cominola A, Nguyen K, Giuliani M, Stewart RA, Maier HR, Castelletti A. Data mining to uncover heterogeneous water use behaviors from smart meter data. Water Resour Res 2019;55(11):9315–33. doi:10.1029/2019WR024897.

[153] Goudbeek A, Choo KKR, Le-Khac NA. A forensic investigation framework for smart home environment. In: Proc. - 17th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. 12th IEEE Int. Conf. Big Data Sci. Eng. Trust. 2018; 2018. p. 1446–51. doi:10.1109/TrustCom/BigDataSE.2018.00201.

[154] Alahakoon D, Yu X. Smart electricity meter data intelligence for future energy systems: a survey. IEEE Transactions on Industrial Informatics 2016;12(1):425–36.

[155] M.T. Schmid, M. Pospiech, and C. Felden, "Identification of smart home potentials in Germany," *Proc. - 2015 IEEE 12th Int. Conf. Ubiquitous Intell. Comput. 2015 IEEE 12th Int. Conf. Adv. Trust. Comput. 2015 IEEE 15th Int. Conf. Scalable Comput. Commun.* 20, pp. 1210–5, 2015, doi: 10.1109/UIC-ATC-ScalCom-CBDCom-IoP.2015.220.

[156] Kapade N. Credit based system for fair data sharing in smart Grid. In: 2017 Int. Conf. Comput. Commun. Informatics, ICCCI 2017; 2017. p. 1–5. doi:10.1109/ICCCI.2017.8117689.

[157] Pu Q, et al. Detection mechanism of FDI attack feature based on deep learning. In: Proc. - 2018 IEEE SmartWorld, Ubiquitous Intell. Comput. Adv. Trust. Comput. Scalable Comput. Commun. Cloud Big Data Comput. Internet People Smart City Innov. SmartWorld/UIC/ATC/ScalCom/CBDCo; 2018. p. 1761–5. doi:10.1109/SmartWorld.2018.00297.

[158] Micheli G, Soda E, Vespucci MT, Gobbi M, Bertani A. Big data analytics: an aid to detection of non-technical losses in power utilities. Comput Manag Sci 2019;16(1–2):329–43. doi:10.1007/s10287-018-0325-x.

[159] Sensarma D, Sen Sarma S. Application of graphs in security. Int J Innov Technol Explor Eng 2019;8(10):2273–9. doi:10.35940/ijitee.J1133.0881019.

[160] Yin X, An H. A novel algorithm with reduced mutual information for smart meter privacy protection. In: 2020 IEEE 5th Int. Conf. Cloud Comput. Big Data Anal. ICCCBDA 2020; 2020. p. 265–9. doi:10.1109/ICCCBDA49378.2020.9095718.

[161] Song J, Liu Y, Shao J, Tang C. A dynamic membership data aggregation (DMDA) protocol for smart grid. IEEE Syst J 2020;14(1):900–8. doi:10.1109/JSYST.2019.2912415.

[162] Guan Z, Si G. Achieving privacy-preserving big data aggregation with fault tolerance in smart grid. Digit Commun Networks 2017;3(4):242–9. doi:10.1016/j.dcan.2017.08.005.

[163] Lyu L, Law YW, Jin J, Palaniswami M. Privacy-preserving aggregation of smart metering via transformation and encryption. In: Proc. - 16th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. 11th IEEE Int. Conf. Big Data Sci. Eng. 14th IEEE Int. Conf. Embed. Softw. Syst; 2017. p. 472–9. doi:10.1109/Trustcom/BigDataSE/ICESS.2017.273.

[164] S. Kessler, E. Buchmann, and K. Bohm, "Deploying and evaluating pufferfish privacy for smart meter data," *Proc. - 2015 IEEE 12th Int. Conf. Ubiquitous Intell. Comput. 2015 IEEE 12th Int. Conf. Adv. Trust. Comput. 2015 IEEE 15th Int. Conf. Scalable Comput. Commun.* 20, no. i, pp. 229–38, 2016, doi: 10.1109/UIC-ATC-ScalCom-CBDCom-IoP.2015.55.

[165] Subhani S, Gibescu M, Kling WL. Autonomous control of distributed energy resources via wireless machine-to-machine communication; a survey of big data challenges. In: 2015 IEEE 15th Int. Conf. Environ. Electr. Eng. EEEIC 2015 - Conf. Proc; 2015. p. 1437–42. doi:10.1109/EEEIC.2015.7165381.

[166] Tzafestas S. Ethics and Law in the Internet of Things World. Smart Cities 2018;1(1):98–120. doi:10.3390/smartcities1010006.

[167] Zwitter A. The network effect on ethics in the big data age. In: In big data challenges. London: Palgrave; 2016. p. 23–34.

[168] Kitchin R. The ethics of smart cities and urban science. Philos Trans R Soc A Math Phys Eng Sci 2016;374(2083). doi:10.1098/rsta.2016.0115.

[169] Nunan D, Di Domenico M. Market research and the ethics of big data. International Journal of Market Research 2013;55(4):505–20. doi:10.2501/IJMR-2013-015.

[170] Rawls J. A theory of justice. Cambridge: Harvard University Press; 1971.