Smart home for lawyers: IoT in the home and its implications for the GDPR

De Conca, S.

published in
Tijdschrift voor Internetrecht
2021

document version
Publisher's PDF, also known as Version of record

Smart home for lawyers: IoT in the home and its implications for the GDPR

dr. S. De Conca[1]

The IoT is "A network of items – each embedded with sensors – which are connected to the Internet"[2] and function thanks to the collection and communication of data. It revolves around the idea that everything can communicate every time and everywhere, in a "ubiquitous network".[3] Today, companies market as 'smart' IoT products that are *intelligent*.[4] Thanks to machine learning, they can talk (voice assistants), change the environmental conditions (lamps and thermostats) and personalise their responses to each user. Today's smart devices (hereinafter also indicated with IoTs) are consumer products whose essence not only lies in their interconnectivity but also in their sophisticated learning and personalisation. Smart devices reach their highest functionality in the smart home, where many traditional appliances are replaced with IoTs. Popular smart home devices are: TVs, thermostats, voice assistants, lightbulbs and switches. However, the sector continues to grow rapidly, offering big and small smart kitchen appliances (from fridges to coffee pots), as well as mattresses, toothbrushes, and even children's toys.[5] The smart home is based on the ubiquitous and invisible collection, analysis, and exchange of data, which makes the private sphere more permeable and increasingly visible for the companies that control these devices. This article looks at the application of the GDPR to the smart home.[6] The first part introduces the changes that the smart home has brought to the traditional conception of home, focusing on the expectations of privacy connected to the private sphere. The rest of the article discusses those provisions that are particularly challenged by the IoTs: the fundamental principles of data processing, the DPIA, and the prohibition of automated decisions and profiling with significant impact.

1. Home, Smart Home, and Privacy

Smart homes are houses embedded with IoTs, connected to the Wi-Fi. Through the internet, the devices send data about their status, software, operative systems, usage and users' preferences to the servers of the producers and business partners. IoTs can also share data with each other or with a hub that coordinates and manages them all.

IoTs often support apps, similarly to smartphones. Some apps are developed by the device's producers, others by third-party companies. Figure 1 represents the ecosystem of devices and apps created inside the smart home. It also shows the multitude of actors that, through the smart home, have access to the personal data of the inhabitants.

1. Silvia De Conca is Assistant Professor in Law & Technology in the Amsterdam Law & Technology Institute (ALTI), Transnational Legal Department, Vrije Universiteit Amsterdam. She is the co-chair of the Group 'Human Rights in the Digital Age', part of the Netherlands Network for Human Rights Research (NNHRR) of the Asser's Instituut, and member of the managing team of the Demonstrator Lab of VU Amsterdam.
2. IEEE, *Towards a definition of the Internet of Things*, 2015, p. 10.
3. *ITU Internet Reports 2005: The Internet of Things*, p. 3. The origins of the term IoT are uncertain: some trace back to the end of the 1990's, to a publication by the International Telecommunication Union (ITU), other to a business presentation by one of the founders of the Auto-ID Center at MIT, Kevin Ashton, who also affirms so himself, saying the term helped him combine two topics, the Internet and business, that were surely going to catch the attention of IBM audience. A. Gabbai, 'Kevin Ashton Describes "the Internet of Things"', *Smithsonian Magazine* January 2015, www.smithsonianmag.com.
4. Most likely leveraging the fact that the word 'smart' can be evocative of the intelligence of AI. In the late 1990s, to enable the full potential of the IoT, it was important to pair it with materials capable to automatically react to external stimuli: these latter were called *smart technology. ITU Internet Reports 2005: The Internet of Things.*
5. 'The Smart Home Market in Europe Experienced the Strongest Quarter Ever in 4Q19, but COVID-19 Will Hit the Market in 2020, says IDC', www.idc.com.
6. The IoTs inside the smart home are digital and electronic products that collect, analyse, store, and transfer data concerning users, their homes, their habits and preferences: they process personal data. They do so in Europe, and vis-à-vis European residents and citizens. Based on these circumstances it is safe to assume that the GDPR applies to IoTs unless the data are anonymised (in which case the GDPR no longer applies, at least from the moment of anonymisation).

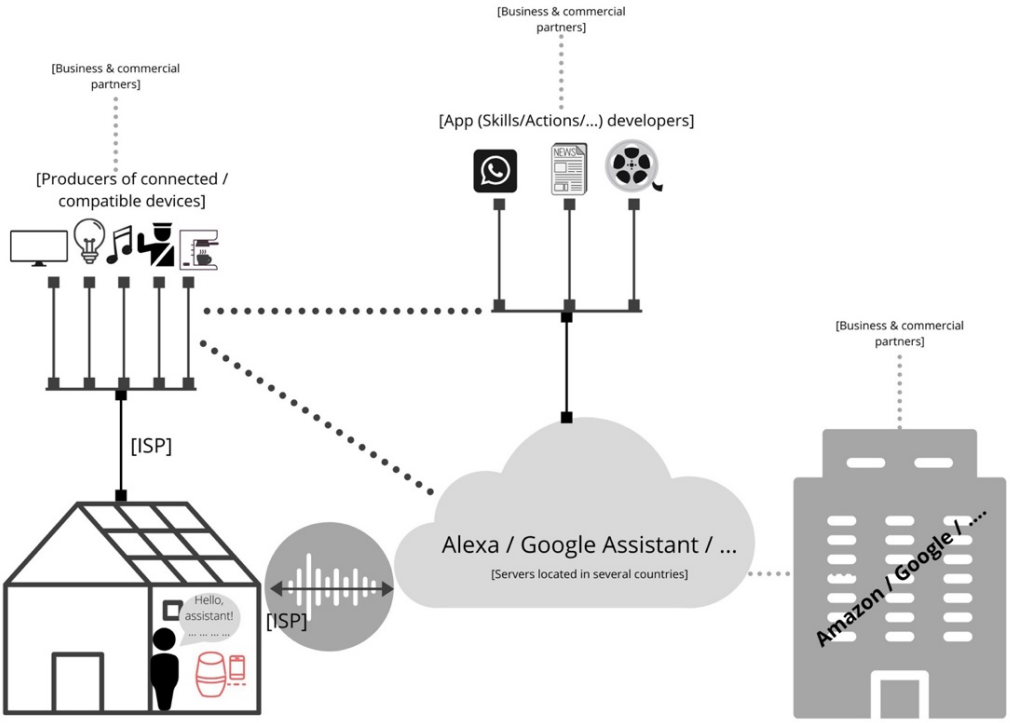

Figure 1: the many devices and apps constituting the smart home. This example specifically shows a voice assistant as the central hub around which other IoTs operate.

This is an important transformation of the home: actions that were once strictly private and remained mostly confined to the individual and family life, are now analysed to gather information about the preferences and behaviours (even future ones) of the inhabitants.

Intuitively, it is easy to grasp that the home holds a special place for individuals and families. According to behavioural science, when individuals settle into a house, even just temporarily, they exercise control and personalise it.[7] Over time, this process creates an emotional connection between the individuals and the house: the house becomes a *home*. The home satisfies the necessities of the inhabitants, is predictable and regulates the interaction with the outside.[8] The inhabitants have certain expectations of privacy[9]: they can cross a room without turning the light on knowing where all the furniture is, unauthorised people cannot get inside, and letters, e-mails, or phone calls are not read or eavesdropped. If an unwanted external interference happens, the inhabitants experience discomfort (as anyone who suffered a home invasion can tell).[10] These interferences matter because the home is a territorial expression of the private sphere, the most inner aspects of life. The private sphere includes the individual's intimacy, thoughts, behaviours, habits, preferences, but also relationships, family, and close friends. Maintaining a private sphere is functional to the development of the identity and dignity of individuals.[11]
The value of the private sphere and of the home (as its proxy) is recognised in the fundamental rights framework of the European Union and in many national constitutions.[12] Protecting personal data is crucial to protect the private sphere: this is the purpose of the General Data Protection Regulation (GDPR), applicable to the processing occurring in the smart home too.[13]

7. I. Altman, 'Privacy: A Conceptual Analysis: Environment and Behavior', *Environment and Behavior* 1976/8, afl. 1, p. 141–181.
8. I. Altman & C.M. Werner, *Home Environments*, Boston, MA: Springer US: Imprint: Springer 1985.
9. The concept of 'expectation of privacy' is also well established in the case-law of the European Court of Human Rights. ECtHR, 'Guide on Article 8 of the European Convention on Human Rights: Right to respect for private and family life, home and correspondence', 2020.
10. P. Korosec-Serfaty, 'Experience and Use of the Dwelling', in: *Home Environments*, I. Altman & C.M. Werner eds, Boston, MA: Springer US 1985, p. 65–86.
11. M.G. Hansson, *The Private Sphere: An Emotional Territory and Its Agent* (Philosophical Studies in Contemporary Culture), Springer Netherlands 2008.
12. J. Kokott & C. Sobotta, 'The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR', *International Data Privacy Law* 2013/3, afl. 4, p. 222–228.
13. As secondary legislation of the European Union, the GDPR contributes to the implementation of articles 7 (Respect for private and family life) and 8 (Protection of personal data) of the Charter of Fundamental Rights of the European Union and article 8 (Right to respect for private and family life) of the European Convention for Human Rights, in horizontal relationships. H. Hijmans,

2. Article 5 and the fundamental principles

Article 5 of the GDPR establishes that the processing of personal data must be carried out in accordance with a set of fundamental principles:

a. Lawfulness, fairness, and transparency of processing;
b. The personal data must be collected for a pre-determined, specific and legitimate purpose (purpose limitation);
c. Only the data adequate and strictly necessary to achieve the above-mentioned purposes must be used (data minimisation);
d. Data must be accurate and up-to-date (accuracy);
e. Personal data must be stored only for as long as they are necessary to achieve the above-mentioned purposes, or else be anonymised (storage limitation);
f. The security and integrity of the personal data must be ensured (integrity and confidentiality).

The principles of lawfulness, purpose limitation, data minimisation, and storage limitation are particularly interesting with regard to IoTs in the smart home.

2.1. Lawfulness

For the processing to be lawful, one of the conditions established by article 6 must apply:

a. The data subject has given consent to the processing based on one or more specific purposes;

and/or the processing is necessary for

b. the performance or entering into a contract;
c. complying with a legal obligation of the controller;
d. protect vital interests of the data subject or another individual;
e. a task carried out in the public interest;
f. the legitimate interest of the controller or a third party, unless such interest is overridden by interest/fundamental rights/freedoms of the data subject.

The various activities carried out by IoTs constitute processing. As such, they must rely on one or more of the grounds above. The analysis below focuses on the two legal grounds more relevant in the context of IoTs: consent and legitimate interest.[14]
Consent is a common legal ground for IoTs. At the first activation of a smart doorbell, TV, or other device, users are asked to consent to the privacy policy (on the device, or via the connected smartphone app).
Consent should be "freely given, specific, informed, and unambiguous" (article 4[11]). For consent to be informed, data subjects must receive all the necessary information concerning the controller, the data collected, the processing and their consequences, as established by articles 12, 13 and 14 GDPR. For it to be specific, data subjects should be able to only consent to some purposes.[15]
It is important that the formulation of the privacy policy or any other form of information provided to a data subject is specific and clear enough to allow data subjects to adequately predict the uses of their personal data and the deriving consequences.

Two criticalities emerge. First, many producers use 'umbrella' privacy policies, relating to all their services and products (as is currently the case with Apple, Amazon, or Google). The French Data Protection Authority (DPA) has ruled Google's umbrella policy incompatible with the principle of transparency, because it fragments and dilutes the information, not allowing data subjects to understand what use will be made of the data, and possible consequences.[16] According to the French DPA, such fragmentation of information makes the consent of data subjects invalid. Google relies on consent for the processing of personal data for targeted advertising purposes. Therefore, targeted advertising was being performed without a valid legal ground: consequently, the French DPA fined Google for 50 million euros.[17]

Second, machine learning technologies, such as those in the smart home, change over time, because the software powering the devices learns new capabilities and new knowledge. As an example, consider that voice assistants can associate a certain voice and manner of speaking to an identified and registered user. Based on this capability, companies are now exploring the possibility to detect the emotional state of a user from their voice.[18] Similarly, face recognition has also opened the way to the exploration

The European Union as Guardian of Internet Privacy: The Story of Art 16 TFEU (Issues in Privacy and Data Protection), Springer International Publishing 2016.

14. The grounds at points (b), (c), (d), and (e) are not interesting for the purposes of this article, either due to their nature of *lex cogens* (the legal obligation being something that controllers must comply with, for instance tax laws), or due to their exceptional nature, which would require a case-by-case evaluation (as in the case of protection of a vital interest and public interest). With regard to the necessity for the execution of a contract, it applies strictly, and only to those data relating directly to the individual entering into said contract. One instance of such case could be the credit card, billing, and identity information collected by a company to make purchases online. This legal ground would concern only that specific purpose (completing the purchasing and billing) and only the data of the specific user making the purchase.
15. E. Kosta, *Consent in European Data Protection Law*, Brill Nijhoff 2013.
16. The French DPA, called CNIL, announced it in the press release of 21 January 2019.
17. An English summary of the CNIL decision is available at www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc.
18. This is not hypothetical. The example is based on a software developed by Amazon called Alexa Hunches: 'Amazon's Alexa can now act on "hunches" about your behavior', *DigiTechNews* 21 september 2018. A similar software is being researched by Google too.

of emotion recognition, using facial expression and muscle movements.[19] When consent is given *a priori*, it presupposes a static environment and the capability to predict implications and risks exactly.[20] The smart home is not static: it learns, while consent is based on an up-front evaluation. The risk is to increase the mismatch between the expectations of the uses and purposes envisioned by the data subject when giving *a priori* consent, and the reality of the downstream implications.

With regard to the legitimate interest of the controller, while it is possible for controllers to rely on it as a valid legal basis for some processing in the case of IoTs, said interest needs to be balanced against the rights and interest of the data subjects. The fact that the IoT operates inside the home sets a high threshold against which the legitimate interests of the controllers is tested. As explained above, the law grants the home extensive protection. This means that the balancing of the legitimate interest of the controllers sees on the other side of the scale the very high privacy expectations existing inside the home. .[21] That is a very high threshold, and some merely commercial interests, such as marketing, are unlikely to prevail. In the smart home, therefore, the legitimate interest might not be the best choice as legitimate ground for some purposes, and consent might play a bigger role – even with all the shortcomings described above.

2.2. Purpose Limitation

The principle of purpose limitation is composed of two main elements: purpose specification and compatible use.[22]
Purpose specification means that the purposes of processing must be established by the controller and communicated to the data subject *before* (or at the same time) the data collection begins.
The purposes must be specific enough to allow data subjects to predict the uses and consequences of data processing. Generic formulas cannot be used: "'improving users' experience', 'marketing purposes', 'IT-security purposes' or 'future research'– without more detail – will usually not meet the criteria of being 'specific"'.[23] This is because purposes that are indicated in a broad manner become a catch-all, allowing the collection of more data that is truly necessary, potentially for multiple uses.
Purpose specification also implies that it is not possible to collect or otherwise process data because they could, maybe, become useful in the future.[24] If a new purpose emerges, there are two options: either said purpose reasonably derives from an existing one, or the purpose must be considered a completely new use of the data. In the latter case, it must have an appropriate legal ground, and data subjects must be informed.[25] The first case is called 'further processing' and its compatibility with the initial purposes must be evaluated on a case-by-case basis (unless the data subject consents). For example, a smart toothbrush might need to keep track of how long individuals brush their teeth, to give them a personal overview of their oral hygiene habits. If the company archives the information for purposes of general medical statistics of the population, that is generally considered a compatible further processing.[26] The compatibility assessment is based on:

a. the formal and substantive connections between old and new purposes (e.g. if the further processes are a logical step, necessary for the original purpose);
b. the context from which the data have been collected, because this affects the expectations that the data subject has about the uses of their data, and the consequences (a certain context might give life to expectations of a stricter confidentiality and, therefore, of more limitations on further processing);
c. the nature of the data (e.g. special categories of data, to which the GDPR assigns special protection);
d. possible consequences on the data subject;
e. possible safeguards (such as encryption or pseudonymisation).[27]

2.3. Data Minimisation

The principle of data minimisation implies that only personal data, which are strictly and directly necessary for the purposes, can be collected. The control-

19. Please note that psychologists and behavioral scientists are divided on the matter: not everyone agrees that it is even possible to detect emotion based on face or voice recognition, and many are skeptical of the accuracy of such software predictions.
20. C.J. Hoofnagle, 'Designing for Consent', *Journal of European Consumer and Market Law* 2018/7, afl. 4, escholarship.org.
21. Article 29 Working Party, 'Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (WP 217)', 2014; G. Zanfir-Fortuna & T. Troester-Falk, *Processing personal data on the basis of legitimate interests under the GDPR: Practical Cases*, 2018, p. 41; I. Kamara & P. De Hert/E. Selinger, J. Polonetsky & O. Tene, 'Understanding the Balancing Act behind the Legitimate Interest of the Controller Ground', in: *The Cambridge Handbook of Consumer Privacy* (Cambridge Law Handbooks), Cambridge: Cambridge University Press 2018, p. 321–352. Many decisions of the Court of Justice of the European Union concerning the legal bases under the Data Protection Directive also offer precious insights about this balancing exercise CJEU: *ANSEF, Joined Cases C-468/10 and C-469/10, [2011] (ECLI:EU:C:2011:777)*; *Breyer, Case C-582/14, [2016] (ECLI:EU:C:2016:779)*; *Fashion ID, Case C-40/17, [2019], (ECLI:EU:C:2019:629)*; *Google Spain, Case C-131/12, [2014], (ECLI:EU:C:2014:317)*; *Puškar, Case C-73/16, [2017] (ECLI:EU:C:2017:725)*; *Rīgas, Case C-13/16, [2017] (ECLI:EU:C:2017:336)*; *Ryneš, Case C-212/13, [2014], (ECLI:EU:C:2014:2428)*.
22. Article 29 Working Party, 'Opinion 03/2013 on purpose limitation (WP 203)', 2013.
23. Article 29 Working Party Opinion 03/2013 (WP 203), p. 15.
24. European Union Agency for Fundamental Rights, 'Handbook on European data protection law', 2018.
25. Article 29 Working Party Opinion 03/2013 (WP 203).
26. 'ICO's Guide to Data Protection', ico.org.uk.
27. Article 29 Working Party Opinion 03/2013 (WP 203), p. 25.

ler must identify exactly which categories of data are necessary to carry out the processing based on the purposes.[28]
If the personal data collected concern information that are irrelevant and not necessary, relate to other individuals, or are collected only because there is a chance that they might become relevant in the future, they are excessive respect to the pre-established purposes. [29]

2.4. Storage Limitation

According to the storage limitation principle, anonymised data can be retained for an indefinite duration, provided that adequate safeguards are in place to prevent de-anonymisation. On the contrary, data for which identification is possible, shall be kept only as long as they are necessary to serve their purpose.[30]
Personal data can be retained until they are necessary not only to the controller, but also for third parties, as long as the storage of the data responds to a legitimate interest, provided that the balancing of the rights of the data subject versus the rights and interests of the third-party results in favour of this latter (and appropriate safeguards are in place).[31]

2.5. Article 5 and the smart home

To see what happens when we apply article 5 GDPR to IoTs in the smart home, consider the case of Alexa using machine learning to understand the command and talk. There is a certain amount of initial data (D^1) collected, such as voice data, useful to distinguish the words pronounced. D^1 is necessary based on the purposes P^1 "provide voice services", and P^2 "provide, troubleshoot, and improve Amazon's Services" (indicated in Amazon's privacy policy, to which the data subjects consent).[32] What about emotion recognition?

The processing necessary to carry out emotion detection would be a new operation, to be evaluated based on:

- the purposes P^1 and P^2;
- potential new purpose (P^3) and its legal ground.

Alexa needs additional data D^{1+x} (where x is the additional data necessary for emotion recognition).
The new data collection should respect the minimisation principle based on purposes $P^{1\text{-}2\text{-}3}$ and should only be retained as long as they are necessary.

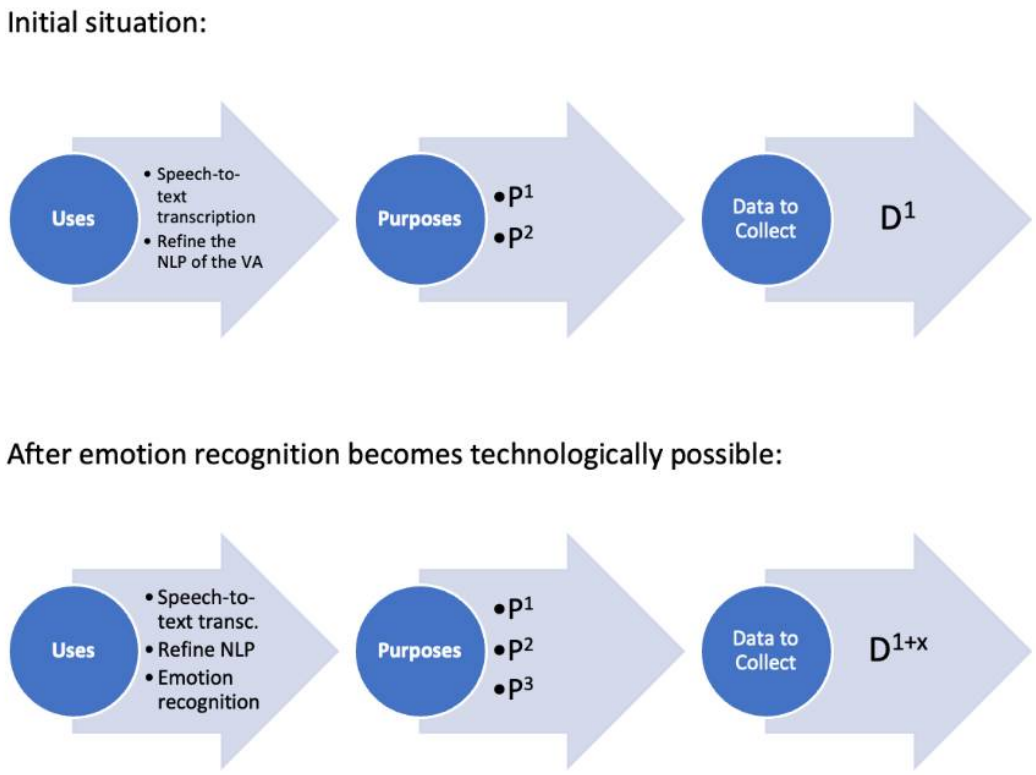

Figure 2: Example of further processing enabled by the AI capability of VAs

28. 'ICO's Guide to Data Protection', ico.org.uk. In combination with the accountability principle it also implies that the controller must be able to demonstrate, via the appropriate documentation, that it only collects the data necessary to the specified purposes.
29. 'ICO's Guide to Data Protection', ico.org.uk.
30. European Union Agency for Fundamental Rights, 'Handbook on European data protection law', 2018.
31. *Manni, Case-398/15, [2017], (ECLI:EU:C:2017:197)*, par. 51–53.
32. 'Amazon.co.uk Help: Alexa, Echo Devices, and Your Privacy', www.amazon.co.uk.

To assess the compatibility of further processing (article 6[4]), it shall also be kept in mind that:

- Alexa operates inside the home, with the abovementioned high privacy expectations;
- Privacy policies indicating generic purposes such as "Provide voice services: When you use our voice services, we process your voice input and other personal information to respond to your requests, provide the requested service to you, and improve Amazon Services"[33] might imply several further processing and connected purposes which an average user is not technologically skilled enough to envision. If data subjects are told by the IoT producers that emotion recognition allows for more accurate personalisation, they might not be able to deduce that advertising is also included, and that a certain emotional status makes an individual more vulnerable to some products or behaviours. The information provided in that case is not in line with the requirements of the GDPR.

Lastly, there is the potential risk that the personal data of the users are necessary for an indefinite period due to the constant evolution of the 'brain' of the IoTs. This appears to be the case with the voice data smart speakers' users[34]: all the communications between users and smart speaker are recorded and stored via cloud servers. These logs can be deleted using the smart speaker app but the companies claim the deletion can cause the smart speaker to be less efficient and personalised. Potentially, Amazon and Google would need to store the voice logs of the users for an indeterminate time, as long as the users maintain an Amazon or Google account connected to the Alexa or Google Home app. The logs are inherently not anonymous since they are connected to the account of the user. The risk is that the use of machine learning leads to a perpetual storage of large amounts of identified or identifiable data.[35]

3. Controllers and processors in the smart home

According to article 4 GDPR, the controller is: "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data". The processors are those natural or legal persons that materially carry out the processing – handling the personal data – on behalf of the controllers and following their instructions.

Means and purposes shall be intended as the "how" (technical and organisational measures, and the essential and non-essential elements)[36] and the "why" of the processing. The interpretation of the word "determine" has raised several doubts in the past. According to the EDPB: "the word "determines" means that the entity that *actually exerts* influence on the purposes and means of the processing is the controller"[37] [emphasis added]. The controller must exercise influence on both the purposes and means in order to be qualified as such, and the purposes and means must be eschathologically connected to the processing of the personal data.[38]

The GDPR expressly considers the possibility of multiple controllers, identified based on a factual evaluation under article 26 (joint control).[39] Based on the interpretations given by the Court of Justice of the European Union (CJEU) in the famous Wirtschaftsakademie, Jehova Witness, and Fashion ID cases[40], and on the European Data Protection Board (EDPB) guidelines on the matter, joint control can be found in two scenarios: one in which there is a shared, common intention among the controllers (common decisions). Another one in which the decision of the controllers on the purposes and means are not common but complement each other (converging decisions).[41] Joint controllers are bound by joint and severe liability, but the responsibility is allocated among controllers based on the factual control they exercise, not necessarily equally. If one controller only determines certain stages of the processing, it will be responsible for the GDPR compliance for that specific stage. This division of the processing activities into various stages is consolidated in the case-law of the CJEU, that has consistently applied it as a way to define the boundaries of the responsibility of controllers and processors, and to simplify the cases of multiple controllers.
The EDPB affirms that to identify a controller it is necessary to answer the questions "why is this pro-

33. 'Amazon.co.uk Help: Alexa, Echo Devices, and Your Privacy', www.amazon.co.uk.
34. A. Ng, 'Amazon Alexa transcripts live on, even after you delete voice records', www.cnet.com.
35. 'EDPS, TechDispatch #1: Smart Speakers and Virtual Assistants', edps.europa.eu, 19 juli 2019.
36. ""Essential means" are closely linked to the purpose and the scope of the processing and are traditionally and inherently reserved to the controller. Examples of essential means are the type of personal data which are processed ("which data shall be processed?"), the duration of the processing ("for how long shall they be processed?"), the categories of recipients ("who shall have access to them?") and the categories of data subjects ("whose personal data are being processed?"). "Non-essential means" concern more practical aspects of implementation, such as the choice for a particular type of hardware or software or the detailed security measures which may be left to the processor to decide on" 'EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR' 2020/38. The qualification of controller is reasonably assigned to those actors having a determining influence on the purposes and essential means (while the non-essential means can, for instance, be left to the processors)
37. 'EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR' 2020/29.
38. 'EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR' 2020.
39. European Union Agency for Fundamental Rights, 'Handbook on European data protection law', 2018.
40. Respectively CJEU: *Fashion ID, Case C-40/17, [2019], (ECLI:EU:C:2019:629)*; *Jehova Witness, Case C-25/17, [2018], (ECLI:EU:C:2018:551)*; *Wirtschaftsakademie, Case C-210/16, [2018], (ECLI:EU:C:2018:388)*.
41. 'EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR' 2020/53.

cessing taking place?" and "who decided that the processing should take place for a particular purpose?"[42]. Consequently, a party might be a controller based on the sole fact that their actions cause the processing of personal data. In this case, the party acts as a facilitator, starting the processing. Finally, in order to be a controller, a party needs not have access to the personal data that are processed.

3.1. Who are the controllers in the smart home?

In the smart home, the presence of several controllers and processors is the norm: each of the actors represented in Figure 1 is a controller and so is the Internet Service Provider.
According to the CJEU, each company is responsible for one or more processing activities (a stage), such as the collection of the data, their storage in the cloud, the processing to personalise the services, or that necessary for advertising, etc. Some might be responsible for the entirety of the processing, because they factually control it all (for instance most of the processing activities are under the control of the smart speaker producer, due to the vocal interface).[43]

Here we notice one peculiarity of the smart home: besides controllers, the companies can also be each other's processors. Consider Amazon, controller for the data collected and processed by Alexa. Alexa supports thousands of apps. The developers of such apps can be controllers for their own parts of the processing, and can also process data on behalf and upon instruction of Amazon, therefore being also its processors. At the same time, Amazon sells web services to the app developers, such as cloud storage. For those services, Amazon can be the processor of the app developer. App developers need access to Amazon's API to create apps compatible with Alexa; they have no choice but to purchase Amazon's web services and accept all the contractual terms and limitations imposed by Amazon. This circumstance, as explained below, makes them controllers for the GDPR, but factually not completely in control.[44]

If this example appears more confusing than helpful, it is because the reality of appointing controllers and processors in the smart home based on the CJEU's idea of dividing the processing into stages, *is* confusing.
Each company is dependent from one another because of how the hardware and software work and due to business agreements. The technological interdependence in the smart home does not sit well with the division of the processing into stages. Based on the factual reality, it would be more appropriate to avoid the division into stages, considering the processing as a whole.[45] As an example, consider a smart TV: it collects data on the users and their watching habits (and, if it has sensors, images and voices). The producer uses the data to deliver a personalised service, improve the algorithms, and profile for advertising. Each purpose can be used to identify one processing operation (consisting of different activities). The smart TV producer is a controller for such processing. If the smart TV supports apps, for instance to play videogames, the developer of the videogame app uses the data collected by the smart TV to deliver a personalised service, improve the game, and sell data to advertisers. The app developer is a controller for the entire processing referred to these other purposes. In identifying the app developer's responsibility it is necessary to consider the contractual terms imposed by the smart TV producer. This approach avoids splitting the processing into smaller and smaller stages in an effort to identify who controls what, and considers that some controllers act as gatekeepers of the data through technological and contractual arrangements; they have a primary position and should, therefore, be the main addressees of the obligations contained in the GDPR. This does not mean that app developers and other producers are not controllers under the GDPR. They are, but their responsibility must be evaluated taking into account the fact that their control is limited by their dependance from the primary controllers. DPAs, national courts, and the CJEU should consider this when assessing their compliance with the GDPR, and especially in calculating possible fines.

The reality of the smart home challenges the interpretation of the CJEU also with regard to the owners of IoTs. The inhabitants of a smart home are data subjects, since it is their data being processed by the IoTs. However, by using a smart security camera, or activating a smart speaker during a dinner with friends, the owners facilitate the processing of the personal data of their guests (such as their image or voice). Because the CJEU and EDPB affirm that the 'facilitators' of the processing are controllers, the owners of some IoTs might find themselves in the difficult position of being controllers vis-à-vis their guests.[46] The implications could be significant: the IoT owners would have to comply with the GDPR's obligations, and be held accountable for it. They would have to esure the respect of the data subject rights of their guests, for instance granting them the right to access their data, rectify them, erase them, and so on. Provisions such as the transparency and information obligations, even the obligation to en-

42. 'EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR' 2020/29.
43. S. De Conca, 'Between a rock and a hard place: owners of smart speakers and joint control', *SCRIPTed* 2020/17, afl. 2, p. 238–268.
44. This is based on an analysis of the services offered by Amazon Web Services and of the API that developers must use to create apps and products compatible with Alexa 'Amazon Web Services (AWS) - Cloud Computing Services', aws.amazon.com.
45. And would also be more in line with the letter of the GDPR that does not include different 'stages' of processing.
46. S. De Conca, 'Between a rock and a hard place: owners of smart speakers and joint control', *SCRIPTed* 2020/17, afl. 2, p. 238–268.

sure the security of the data processing, could potentially apply. For an average user with no technological expertise, these can easily degenerate into impossible tasks.

One factor that could mitigate the obligations of the owners of IoTs is that the processing of the guests' data occurred in the context of private or family activities. This could be enough to configure the so-called household exemption (article 2[2][c] GDPR). The household exemption limits the material scope of the GDPR to the commercial processing of personal data, excluding those activities that fall within the private and family life of an individual (such as having a digital contact list of friends and family, or entertaining e-mail correspondence, for instance). In simpler words, with the house exemption the GDPR does not apply. However, the household exemption does not apply if the data are collected outside the house, from hallways or streets (as those would be public).[47] Smart security cameras, for instance, collect and process data outside of the home: in this case, the household exemption does not apply. Similarly, if the sensors of a device are powerful enough to collect data – for example sounds – from the neighboring houses, the household exemption might not apply.
The application of the household exemption to online activities is also unclear. If, for instance, an individual shares personal data of others on social media, the household exemption might not apply, especially if the profile is public or has a significant amount of contacts (how many contacts is unknown).[48] A recent Dutch case shows the implications of this interpretation: a grandmother posting pictures of the grandchildren on Facebook was considered a controller and the household exemption was not applied, because her profile was open.[49]
In the cases above, the position of the owners of IoTs vis-à-vis their guests, remains unclear, with the possibility of the owners being controllers while, at the same time, having little-to-no factual control over the devices, besides deciding to turn them off. In the absence of a clear position of the EDPB or CJEU, it could be useful to develop a new etiquette: when guests enter the house, the IoT owners should inform them of the presence of IoTs in the home, offering to turn the devices off or temporarily deactive them (for example, by using the mute button on a smart speaker), where possible. This solution, however, only intervenes at the level of social customs and, as such, requires time to consolidate as a new habit. Furthermore, while it might prevent conflicts among friends, this solution does not exclude the possibility that IoT owners become controllers under the GDPR: that is a legal uncertainty that remains to be solved by national DPAs, the EDPB, or the CJEU.

4. DPIA

Controllers must carry out a Data Protection Impact Assessment (DPIA) under article 35 GDPR, when the processing is likely to pose high risks to the rights and freedoms of data subjects, based on its nature, scope, context and purposes.

A DPIA is a "systematic process for evaluating the potential effects on privacy and data protection of a project, initiative, proposed system or scheme and finding ways to mitigate or avoid any adverse effects".[50] The DPIA reflects a risk-based approach: it is a preliminary reflection, carried out by the controller, on the risks implied by the processing, the relationship of said risks with the purposes and methods of the processing, and possible mitigating measures. A DPIA is particularly recommended when using new technologies, and it is mandatory when it involves a systematic and extensive evaluation of individuals based on automated decisions of processing, or processing on large scale of sensitive data (article 35[3] GDPR).[51]

IoTs make the private sphere more permeable, taking away control from the inhabitants. Individuals share their personal data with less awareness inside the home, due to the perceived safety of the environment. If the IoTs are equipped with voice or face recognition, they use large quantities of biometric data for identification, falling within the special category of data (article 9 GDPR). This aspect might be worsened by the ongoing development of emotion recognition, that might increase the vulnerability of the individuals inhabiting the smart home.[52] Finally, in the smart home individuals are surrounded by an environment that is based on personalisation and optimisation. This can have consequences in terms of systemic discrimination (as explained below) and manipulation, due to behavioural design techniques that aim at maximising user engagement, or nudging users towards certain products or services.[53]

All these circumstances point in the direction of a DPIA being necessary for IoTs (some of which even

47. CJEU, *Ryneš, Case C-212/13, [2014], (ECLI:EU:C:2014:2428).*
48. CJEU, *Buivids, Case C-345/17, [2019], (ECLI:EU:C:2019:122).*
49. Rechtbank Gelderland 13 May 2020 (*ECLI:NL:RBGEL: 2020:252)1.*
50. P. De Hert & V. Papakonstantinou, 'The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals', *Computer Law & Security Review* 2012/28, afl. 2, p. 130–142.
51. P. Voigt & A. von dem Bussche, *The EU general Data Protection Regulation (GDPR): A Practical Guide*, Springer 2017; C. Quelle, 'The "Risk Revolution" in EU Data Protection Law: We Can't Have Our Cake and Eat It, Too', in: *Data protection and privacy: the age of intelligent machines*, R. Leenes e.a. eds. (Computers, privacy and data protection), Oxford ; Portland, Oregon: Hart Publishing 2017.
52. Some authors also point out that the female characterisation of some IoTs, such as smart speakers, can negatively affect women, perpetrating discriminatory stereotypes. N.N. Loideain & R. Adams, 'From Alexa to Siri and the GDPR: The gendering of Virtual Personal Assistants and the role of Data Protection Impact Assessments', *Computer Law & Security Review* 2020/36, p. 359-366.
53. S. De Conca, *The Enchanted House: an analysis of the interaction of intelligent personal home assistants (IPHAs) with the private sphere and its legal protection*, (diss. Tilburg University, Tilburg: 2021).

constitute a new technology). It is reasonable to assume that the main producers, such as Amazon, Apple, Google, Phillips, or Sony, have a general obligation to carry out a DPIA for the processing activities connected to their services, and that such DPIA includes their IoTs too. It is also reasonable to assume such DPIAs already exist, however they are not disclosed publicly: in the context of the smart home the DPIAs could shed light on the way in which the processing takes place, how the manufacturers consider the processing proportional and necessary (in relation to its purposes), the risks involved, the implications on the rights and interests of their users, and which safeguards have been taken.

5. Profiling

Many producers of IoTs carry out profiling and/or automated decisions, to personalise their services on the users. IoT producers and developers can also develop profiles of their users for advertising and marketing purposes, or to sell to third parties.

The GDPR contains two disciplines concerning profiling and automated decisions: the general one, applicable to all automated decision-making and profiling (as they imply processing of personal data), and the specific discipline of article 22, applicable to automated decisions and profiling activities solely based on automated processing and producing legal or similarly significant effects.[54]

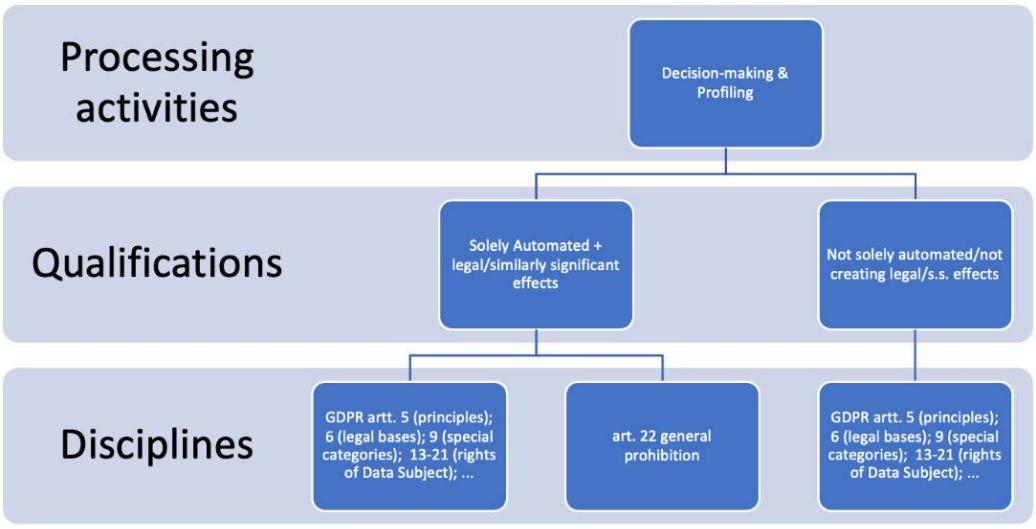

Figure 3: a visual summary of profiling and automated decisions in the GDPR

Profiling is an evaluation of the individual, in the light of a pre-established purpose[55] "in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements" (article 4[4] GDPR). Automated decision making consists of deciding based (solely) on technical means, without any concrete human intervention; it can follow from (or be based on the results of) profiling or be independent from it.[56]

5.1. The general discipline for profiling

The GDPR applies to profiling and automated decisions as it would apply to any other form of processing: the fundamental principles, legal grounds for the lawfulness of processing, transparency and information of the data subjects, their rights, etc., are all applicable provisions. The only difference is that in applying such provisions it is necessary to consider the specific risks deriving therefrom. For instance, regarding consent as a legal basis for profiling, controllers need to:
"*show that data subjects understand exactly what they are consenting to, and remember that consent is not always an appropriate basis for the processing. In all cases, data subjects should have enough relevant informa-*

54. Article 29 Working Party, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (WP 251rev.01)', 2018.
55. I. Mendoza & L.A. Bygrave, 'The Right Not to Be Subject to Automated Decisions Based on Profiling', in: *EU Internet Law: Regulation and Enforcement*, T. Synodinou e.a. eds, Springer 2017.
56. If a human is involved merely into formalizing or applying a decision taken by a machine without intervening on it (or by simply routinely approving all the decisions), the decision-making process would still be considered automated. Article 29 Working Party, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (WP 251rev.01)', 2018.

tion about the envisaged use and consequences of the processing to ensure that any consent they provide represents an informed choice".[57]
For the use of legitimate interest as a legal ground, the mere convenience (in terms of costs or time) of profiling does not constitute a legitimate interest, and factors such as the intrusiveness of the profiling (and the underlying surveillance and tracking activities) shall be taken into consideration when balancing the rights of individuals with the interests of controllers and third parties. In other words, not all the processing activities connected to profiling can be justified by the legitimate interest, due to the intensive profiling carried out by IoT producers. The necessary balancing exercise between the interests of the controller and those of the data subjects must consider that the data were collected inside the home – the sanctuary of private life – where privacy expectations are very high. While the intrusive processing necessary for profiling might be justified in the light of providing a service, it might not be the case of marketing and advertising activities.[58]

5.2. The special discipline of Article 22 GDPR

The special discipline of article 22 GDPR applies if the profiling or automated decisions are entirely carried out without human intervention and create legal or similarly significantly affecting effects. Legal effects are those detrimental for fundamental rights and freedoms, civil rights, legal status, contracts and obligations (e.g. the cancellation of a contract, denial of welfare benefit, or denial of citizenship).[59]
'Similarly significantly affecting effects' means that even if the legal position of the data subject is not affected, a certain area of life is impacted in a way that, due to its importance, can be compared to that of a legal status[60]. This occurs if, for instance, the profiling or automated decision is detrimental to "circumstances, behaviour or choices of the individuals concerned"[61], presents effects that are prolonged or even permanent, or results in discrimination. Profiling or decisions concerning financial circumstances, health services, employment, education, or price differentiation that impedes the purchase of goods or services fall under article 22 GDPR, while it is not clear whether emotional effects (which might derive from a discriminatory automated decision, for instance) might also be part of the provision.[62]
To determine whether it has significant effects, targeted advertising must be evaluated based on, among others, the expectations of the data subjects and the intrusiveness of the tracking, especially if it followed data subjects across different services, websites or devices.[63]

Under article 22, profiling/automated decisions resulting into legal or similarly significant effects are prohibited, with a set of (narrowly interpreted) exemptions. The general prohibition does not apply if the automated decision or profiling is: i) necessary to enter into, or for the performance of, a contract; or ii) based on the explicit consent of the data subject. In those cases, the controller must establish appropriate safeguards to protect the fundamental rights and freedoms of the data subject. Among these safeguards, article 22(3) expressly mentions the right of data subjects "to obtain human intervention" (so called *human in the loop*), to contest the decision and express their point of view.
If the automated decision is based on sensitive data, the prohibition can be derogated only if three conditions are met: i) the processing is carried out based on one of the abovementioned exemptions; ii) the data subject has given consent; iii) appropriate safeguards exist.
Under articles 13, 14 and 15 GDPR, the controller must provide "meaningful information about the logic"[64] of the automated decisions or profiling and an explanation of the envisaged consequences and the significance of the decision. [65]

57. Other specifications are provided with regard to other legal bases, such as contract and legal interest. Article 29 Working Party, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (WP 251rev.01)', 2018, p. 13.
58. idem
59. idem
60. The impact should be "non-trivial". I. Mendoza & L.A. Bygrave, 'The Right Not to Be Subject to Automated Decisions Based on Profiling', in: *EU Internet Law: Regulation and Enforcement*, T. Synodinou e.a. eds, Springer 2017.
61. Article 29 Working Party, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (WP 251rev.01)', 2018, p. 21.
62. Article 29 Working Party, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (WP 251rev.01)', 2018; I. Mendoza & L.A. Bygrave, 'The Right Not to Be Subject to Automated Decisions Based on Profiling', in: *EU Internet Law: Regulation and Enforcement*, T. Synodinou e.a. eds, Springer 2017.
63. It should be noted how this interpretation of the Working Party addresses only certain forms and uses of behavioural advertising, not behavioural advertising in general. M. Kaminski, 'The Right to Explanation, Explained', *Berkeley Technology Law Journal* 2019/34.
64. Article 29 Working Party, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (WP 251rev.01)', 2018.
65. A debate has developed among experts, concerning the interpretation of 'meaningful explanation'. For an overview, see M. Kaminski, 'The Right to Explanation, Explained', *Berkeley Technology Law Journal* 2019/34. 'Meaningful information about the logic' of a decision can be interpreted as including the entire dataset used to train the machine learning software, or even a technical explanation of the rules at the basis of the programming of the software. These provisions aim at putting data subjects in the position to exercise their rights under the GDPR. Data subjects must be able to understand, from said information, the possible implications of the data processing for their rights and interests. In this sense, meaningful information cannot be limited to technical knowledge but should include information about the underlying purposes and incentives of the controller, including the advantages deriving to the controller from the decision, and a clear indication of the criteria used to identify which decisions would be considered correct and optimal, and which would be discarded by the controller. Some authors include in said information also

5.3. One big decision or many small ones? Article 22 and the smart home

Inside the smart home, IoT devices may take decisions regarding small, trivial, daily activities, such as entertainment or grocery shopping. On its own, each of these small decisions seems unlikely to have significant detrimental effects on individuals. These decisions are the result of profiling, as such subject to the general regime of the GDPR, but due to the lack of significant impact they fall outside of the scope of article 22.

There is also another aspect to discuss. With the smart home revolution, does the assumption that one single decision/profiling generates significant detrimental effects still hold?-
Imagine being subject to price discrimination on a consistent amount of smaller daily purchases for medium and long terms (one year, five years, or more).
The price discrimination might not be significant on each purchase, but the accumulation of many purchases can add up to consistent amounts. And the price discrimination might not be performed by one actor, but by all those depicted in Figure 1. In the smart home, the individual lives inside an environment (both online and offline) that is constantly adjusted and potentially optimised... but that might optimise harms too. Multiple, frequent, small decisions on adjusting the temperature of a room, or the price of goods purchased, can add up in the medium- and long-term leading to important effects on individuals, their agency, and their property.

The possibility of a cumulative effect of multiple small, automated decisions/trivial profiling is currently not contemplated by the lettering nor the interpretation of article 22. With the diffusion of IoT, however, this might become a more pressing issue, that requires an evaluation not only of the technical aspects, but also of commercial, business, and sector-specific practices.

Some indications concerning the interpretation of article 22 might come from the Court of Amsterdam, in a case concerning not IoTs, but Uber. A group of drivers from the United Kingdom has brought a lawsuit against Uber's European subsidiary, in front of the competent Court of Amsterdam.[66] The claimants affirm that Uber's algorithm profiles drivers based on certain datapoints (e.g. distance from the user, rating of the drivers, etc.). Based on the outcome of the profiling, the software allocates the rides among the drivers (automated decision). The datapoints and the logic of the profiling have not been disclosed by the company to the drivers (not even after an official access request). With the lawsuit, the drivers hope to bring transparency and clarity on the profiling and decisions determining their jobs and incomes. While the technology is different, this case can offer the occasion for clarifying the application of article 22 to cumulative effects and be a precedent for several other technologies and services, IoTs included.

6. Conclusions

The smart home transforms the physical container of the private sphere, harvesting the spontaneous and private behaviours of individuals for data on a daily basis.[67] The GDPR plays a fundamental role in protecting the rights and interests of the smart home inhabitants. The IoTs technological features and the sector's business practices exacerbate some existing data protection issues and pose new ones. This article offered a bird-eye view of a selection of challenges to the GDPR as applied to smart homes, focusing on: the difficulty to identify controllers and processors due to the many, interdependent, devices; the risk that IoT owners become controllers under the GDPR for the personal data of their guests; the potential perennial storage deriving from ever-changing machine learning; the necessity of a DPIA due to the profound risks to the private sphere deriving from IoTs; and the shortcomings of the prohibition of automated decisions and profiling in the context of a myriad of small daily decisions in the smart home ecosystem.
The issues presented herein are only the beginning: the sector grows rapidly, and with it the possibilities for companies to surveil and predict individual behaviours inside their private sphere. As anticipated by Bill Gates in 2007, soon there will be "a robot in every home"[68]: a scrutiny, by European and national authorities, of IoT and their compliance with the GDPR is becoming not only auspicable, but most likely inevitable.

---

an explanation of the business model of the controller. G. Malgieri & G. Comandé, 'Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation', *International Data Privacy Law* 2017/7, afl. 4, p. 243–265.

66. N. Lomas, 'UK Uber drivers are taking the algorithm to court', social.techcrunch.com, 20 July 2020.
67. Z.A. Papacharissi, *A Private Sphere: Democracy in a Digital Age*, Polity Press (Cambridge) 2010; J.E. Cohen, *Configuring the Networked Self. Law, Code, and the Play of Everyday Practice*, Yale University Press 2012; M. Hildebrandt, 'Privacy as Protection of the Incomputable Self: From Agnostic to Agonistic Machine Learning', *Theoretical Inquiries in Law* 2019/20, p. 83–121; Zuboff, Shoshana, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, Public Affairs 2019.
68. B. Gates, 'A robot in every home', *Scientific American* January 2007.