Affecting the Right of a Private Life Through the Use of the Virtual Assistance

Camelia Daciana Stoian*

Abstract:

Where and how a gadget "lives", who is perfecting it and who is defining it as being always "up to date" or "state of the art", what involves this continuous management process and based on what criteria this is happening, these are the questions that many of us did not address, or did not so much bother to show some concern as long as the device delights us through its quick response time when it comes to organising the agenda for the day or finding a route, basically through everything that it does that contributes to supporting a daily activity and that relieves us from an extra effort. However, relatively recent, as European citizens or adhering to this entitlement, this also strengthens the rights that come related to the level developed by understanding, by the actual perception of the notion of "processing", by reporting to the "restriction of processing", by "creating profiles", by "data tracking systems", by "personal data", or by "consent".

This very article represents an analysis meant to contribute to the awareness but especially to the prevention, by means of adequate information on the rights that we can exert in order to avoid any harm to our private life, thus being and remaining the rightful owners in control of the possibilities of broadcasting any kind of information that identifies us directly or indirectly.

Keywords: form of automatic processing, the right to prior information, the right of access, the right of "being forgotten", the right of restricted processing, violation of private life

Exerting the Right of Ownership over a Gadget

Virtual assistants are mobile goods perceived as a useful and exiting purchase under the condition that they become, at least for the first glance, an exclusive property. A wristwatch that indicates the number of steps performed daily, that measures our blood pressure, blood sugar level, pulse or indicates the route, which warns us if we are stationary for a long period of time or a gadget that can respond to our daily curiosities or relaxes us by playing our favourite song, entitles us to be the proud owners of the right to own, to use and dispose of it in an understandable way as being exclusive and absolute. But, do we know

* Lecturer, PhD, "Aurel Vlaicu" University of Arad, office@avocat-stoiancamelia.ro

the limits of this exercise of such a right of ownership, or have we been properly informed in advance of this particular fact before paying the price? Are we actually aware of the way through which the prompt answer to our question is formed, the categories of information provided about us through which the experience and functions of the device are improved in our interest or who is gathering and processing those data that *evaluate certain personal aspects*? In what way and to what extent does the device recognize what we want and give us the desired answer? All these questions should be included in some preliminary pieces of information, and under any circumstances they should not be part of an automatic processing decision, this also includes creating new profiles that might affect us and upon which we do not have any control right.

In order to reach the end of this idea it is necessary to also know who must realize these prior pieces of information and point out accurately the exact moment of fulfilment. Is the producer or are the legal entities that intermediate(s) by offering for sale the virtual assistance, as long as the networking of the procurement procedure we carry out directly with them? Analysing from the point of view of the provisions of the EU Regulation 679/ 2016, we find out that the right to obtain a prior piece of information is exercised by reference to the "operator". "The operator" is defined as being an individual or legal person, who establishes the purposes and means of processing our personal data, and, in this case, definitely, the producer is in fact the only one who can intervene inside a software in order to provide improved answers. Beside this, us as well, all the owners of such devices, we can only address the operator in order to obtain a confirmation regarding the processing of certain personal data that belong to us, regarding the indication and explanation of the purposes of processing, the type of information targeted, indicating the persons who collect these data, if they were or are being divulged, where they are stored, the period for which they are expected to be stored or especially the existence of an automated decision making process including creating new profiles. However, we repeat ourselves, our interaction is only with the legal person who distributes these gadgets through sales, a person who does not effectively manage the collection part by capturing the voice recordings carried out inside the house, the car, the work place, a person who does not have as a result the role of the "operator" by the means of guaranteeing the right to request the deletion or restriction of the processing of these personal data referring to us or to the right to oppose the processing.

Thereby, we could state, at least a few questions are born with a sensitive role regarding the protection of personal data: *What is the*

procedure for obtaining accurate prior information before selling the virtual assistant and by whom?, Does it represent a touch on the private life, capturing, listening and audio recording a person situated in a house or a room, or recording the correspondence with their own personal virtual assistant in order to improve its function?, Does the complete and exclusive ownership of the device allow operation on its software in the absence of prior information and, as a consequence, on the absence of the owners' agreement?, Why is everyone talking about the "client's security and confidentiality", as long as they are not informed about the constant audio surveillance or the possibility that they are being recorded before even buying a smart device?[1]

The Description of the Status of Fact by Reference to the Incident Legislation

As far as the status of fact is concerned, we appreciate that we find ourselves in a moment when we oscillate between the idea of accepting that we are being monitored but we do nothing for that, by putting in foreground the utility of a smart speaker and the idea of opposing monitoring without even having a procedure in hand in this regard. After all, in an overall analysis of the incident legislation area we can only puzzle together a corroboration of several normative acts and appeal to the somewhat outlined jurisprudence of the European Court of Justice.

For the purpose of the provisions of the EU Regulation no. 679/ 2016 referring to the protection of the individuals in regard to the processing of personal data and looking at the free movement of those data[2], the content of the term "processing" covers all the operations that manage personal data or are concentrated on the personal data of a certain individual, being reflected in actions such as collecting information by listening and recording, extraction, annotation, use in any way of those pieces of information, disclosure via transfer or dissemination, making it available in any way to another individual or

[1] Retrieved from the site:
https://www.bloomberg.com/news/articles/2019-04-10/is-anyone-listening-to-you-on-alexa-a-global-team-reviews-audio: *We take seriously the security and confidentiality of our clients*, declared a spokesperson person from Amazon in a declaration sent by e-mail. *We only annotate an extremely small sample of Alexa's voice recordings in order to improve customer experience. We have strict technical and operational guarantees and we have a zero tolerance policy for abuses in the system. The employees do not have direct access to the information that can identify the person or the account. All the information are treated with high confidentiality and we use a multiple authentication to restrict access, encryption of the services and audits of our control environment.*

[2] Adopted in Brussels, 27 April 2016 and published in the Official Journal under the number 119L from 4th May 2016.

legal person, or even by storing these pieces of information. In close correlation with all legal activities related to everything that can sum up any type of processing of personal data, automated or not, the right to the "restriction of processing" *is sealed and can be manifested under the conditions in which all the operations listed unlimited above are known or aware.*

The knowledge of the existence of processing activities concerning everything that identifies us directly or indirectly, specific elements to our identity whether physical, genetic, mental or occupational, professional, economic, cultural or social, underline a high degree of importance especially when we are considering the *possibility of creating certain profiles regarding us*. "Creating profiles" implies, according to the invoked Regulation, *any form of automatic personal data processing that consists of using personal data to evaluate certain personal issues referring to an individual, especially to analyse and predict performance aspects regarding performance at work, financial situation, health, personal preferences, interests, reliability, behaviour, location of the individual or his traveling*[3]. Therefore, creating a profile is done through a characterization of ourselves, by highlighting of some personal aspects in order to facilitate for the operator the accomplishment of predictions in regard to our future expectations from a certain smart speaker, which determines taking some decisions that do not concern us directly, and over which we do not have any control rights. The decisions determined by automatic means are allowed according to the legislation in force, only under the condition of insuring the possibility of caring out a contract that has been finalized or based on the expression of an unequivocal accord and in total awareness of the case by underlining the compliance at organizational and technical level of all the rights belonging to us. The decisions that are determined by using non-automatic means, of some human factors, should follow even more so the same procedure initiated by an adequate prior piece of information.

The non-regulation by the manufacturer, a legal person of European citizenship or not, of a procedure of information, complete, explicit and prior for the future users of smart gadgets in the European Union, places him in the position of violating some normative acts in force, such as the

[3] Article 4, line 1, point 4, from the EU Regulation no. 679/ 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

Charter of Fundamental Rights of the European Union[4], the European Convention of Human Rights[5] or any other international act that protects human rights.

At national level, let us not forget, from reasons justified by the relations encountered in the society of the latest years and taking act of the European context, starting the entry into force of the new Penal Code, the criminal offence "Violation of private life" was regulated in the Article 226. So nowadays the State is forced to guarantee the non-interference of any individuals or legal persons in the private life of another person by incriminating some actions like "capturing or recording of images", "listening by technical means" or "audio recordings of an individual situated in a home or room or outhouse belonging to it or of a private conversation", "the disclosure, broadcast, presentation or transmission, without right, of sounds, conversations or of images to another person or the public". Of course, the smart speaker is not a "person" but behind its image, responsible for managing it there are the decision making factors, human decision makers, one or multiple individuals and implicitly legal entities. The sanctions proclaimed are not to be neglected, consisting of prison sentence or fine and, honestly, we do not want to think of the punishment resulting under the conditions in which it is analysed how many such actions could be on role under the conditions of the "annotation" even involving "an extremely small sample of voice recordings" when reported to a number advertised as high to 100 million users[6].

---

[4] It was proclaimed by the European Commission, the European Parliament and the Council of the European Union on the 7th December 2000, within the Nice European Council.

"***Art. 8: Protection of personal data***:

(1) Every person has the right to the protection of personal data that concern him.

(2) Such data must be treated correctly, for the specified purposes and based on the consent of the person concerned or on the basis of another legitimate reason provided by law. Any person has the right to access the collected data that concern him, as well as the right to obtain their rectification".

[5] Developed by the European Council, it includes the fundamental rights and freedoms, being signed on the 4th November 1950 in Rome. "***Art. 8 The right of respecting the private life and family rights***: Every person has the right of respecting the private and family, his home and his correspondence. It is not allowed the intervention of a public authority in the exercise of this right any other way but what is provided by law and constitution, in a democratic society, a necessary measure for national security, public safety, countries' economic well-being, defending order and preventing criminal acts, health and moral protection, freedom and rights of others".

[6] https://www.profit.ro/povesti-cu-profit/it-c/100-de-milioane-de-dispozitive-folosesc-asistentul-digital-alexa-18808861.

Any of the actions described, once they have determined a non-communicated data collection that concerns us, therefore illegal, it is correlatively our right to restrict the processing to the same extent as we have the right to obtain the entire effective amount of data collected, of information collected and this even more so as they may even be necessary for example in situations that require the exertion or defending of a right in court, or even proving committing a criminal offence. This last exercise of the right to get exactly the data collected can as well raise new question marks in the conditions in which the smart speaker through the direct correspondent, the human ears involved, can be the witness of committing criminal acts in regards to which they perform an ex officio restriction of access, thus facilitating the birth of new adverse legal consequences.

Moreover, recently via the media institutions it is advertised the fact that with the help of the smart speakers *can have access to data concerning the location of the users*[7]. Thus we consider it useful to exemplify in the context analysed a part of the considerations which were the basis for the invalidation by the European Court of Justice in 2014 of the EU Directive no. 2006/24/CE that imposed the obligation of the states to collect data regarding electronic and telephone communication of its citizens for a period of at least 6 (six) months. This fact is also determined by the idea that governs the application of the EU Directive no. 2006/24/CE in the sense that it was imposed to the providers of communication services to store and ensure the communication to the secrete service structures of all data that are part of the identity of those who are communicating, *the location from where they are communicating as well, in practice all user's locations*[8].

Another important similarity to take note of is that declaring it invalid, rare as a decision itself, was centred as the main motivation *on the idea of inadmissibility of maintaining a legislative act as a directive that determines by application the violation of human rights and "represents a very serious interference in the fundamental rights in respect to private life and protection of personal data's"*[9]. The directive being a legislative act, its invalidation had as a consequence[10] even the

[7] https://www.descopera.ro/lumea-digitala/18104159-echipa-dispozitivului-alexa-poate-accesa-adrese-convorbiri-inregistrari-ale-clientilor.

[8] https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054ro.pdf.

[9] https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054ro.pdf.

[10] The directive 2006/24/EC was implemented at national level by the Law no. 82 from 13th June 2012 regarding the retention of the data generated or processed by the providers of electronic communication networks, the providers of electronic communication services meant for public use, as well as for the modifications and

withdrawal of the internal normative acts of its implementation on national level and consequently the drawing of new limits imposed by conditional respect of the principal of proportionality.

Conclusions

The extent, but especially the seriousness of the interference with the right of respect for privacy and the protection of personal data by reference to the intended purpose depending on the marketing presented for the purpose of distributing for sale some virtual assistants, in the absence of prior information, of adequate guarantees to make proof of limiting any type of abuse, of an effective data protection and of an express consent is a violation of human rights.

Identifying during the research of the factual and legal grounds of the described context, a point of view of Mr. Florian Schaub, assistant professor at the University of Michigan, Faculty of Computer Science and co-author of the study, published in Journal Proceedings of the ACM on Human-Computer Interaction – CSCW, we can say that we embrace the conclusions drawn as follows: "Smart speakers with voice assistants, such as Amazon Echo and Google Home, offer benefits and comfort, but also raise privacy issues thanks to their continuous listening microphones. I studied people's reasons for and against the adaptation of smart speakers, their perceptions and concerns about confidentiality, as well as their behaviours that seek confidentiality around smart speakers. I realized a journal study and interviews with seventeen users of smart speakers and interviews with seventeen non- users. I have found that many non-users have not seen the usefulness of smart speakers or do not trust speaker companies. In contrast, users express some concerns about confidentiality, but their rationalizations indicate an incomplete understandings regarding the risks of confidentiality, a complicated relationship of trust with companies of the speakers and the addiction on the socio-technical context in which the intelligent speakers live. Finally, the current privacy controls of smart speakers are rarely used because they are not well aligned with users needs. Our findings can inform future smart speaker models; in particular, we recommend a better integration of privacy controls in the intelligent interaction of the speakers"[11].

---

completion of the Law no. 506/ 2004 regarding the processing of personal data and the protection of private life in the electronic communication sector. Subsequently, by the Decision of the Constitutional Court no. 440 from 8th of June 2014 it was found that the provisions of the Law no. 82/ 2012 are unconstitutional.

[11] Have a look at https://dl.acm.org/citation.cfm?id=3274371;

REFERENCES:

Decision of the Constitutional Court no. 440 from 8th of June 2014.
EU Regulation no. 679/ 2016.
Law no. 82 from 13th June 2012.
Official Journal, nr. 119L, 4th May 2016.
https://www.profit.ro/povesti-cu-profit/it-c/100-de-milioane-de-dispozitive-folosesc-asistentul-digital-alexa-18808861.
https://www.descopera.ro/lumea-digitala/18104159-echipa-dispozitivului-alexa-poate-accesa-adrese-convorbiri-inregistrari-ale-clientilor.
https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054ro.pdf.
https://dl.acm.org/citation.cfm?id=3274371
https://www.bloomberg.com/news/articles/2019-04-10/is-anyone-listening-to-you-on-alexa-a-global-team-reviews-audio

---

'Smart speakers with voice assistants, like Amazon Echo and Google Home, provide benefits and convenience but also raise privacy concerns due to their continuously listening microphones. We studied people's reasons for and against adopting smart speakers, their privacy perceptions and concerns, and their privacy-seeking behaviors around smart speakers. We conducted a diary study and interviews with seventeen smart speaker users and interviews with seventeen non-users. We found that many non-users did not see the utility of smart speakers or did not trust speaker companies. In contrast, users express few privacy concerns, but their rationalizations indicate an incomplete understanding of privacy risks, a complicated trust relationship with speaker companies, and a reliance on the socio-technical context in which smart speakers reside. Users trade privacy for convenience with different levels of deliberation and privacy resignation. Privacy tensions arise between primary, secondary, and incidental users of smart speakers. Finally, current smart speaker privacy controls are rarely used, as they are not well-aligned with users' needs. Our findings can inform future smart speaker designs; in particular we recommend better integrating privacy controls into smart speaker interaction'.