Iris Online
Journal of Sciences

Iris Publishers

Research Article

The Continuous and Widespread Violation of GDPR in the Personal Communications of European Citizens, Disregarding their Private Lives

Christos P Beretas*

Head professor of cyber security department of Innovative Knowledge Institute (Paris Graduate School), Paris, France

***Corresponding author:** Christos P Beretas, Head professor of cyber security department of Innovative Knowledge Institute (Paris Graduate School), Paris, France.

Received Date: June 06, 2023

Published Date: June 16, 2023

Abstract

In recent years the field of information technology and communication has made enormous progress, one characteristic progress is the ease of systems interconnection of different technologies with other systems that are able to operate automatically and perform automated processes, this has been greatly helped by the technological evolution data compression, data conversion into other formats which aimed to reduce the volume of data and lower prices on storage media and create new storage media. Today, the whole life of a person, that is, all his/her activities can be stored on a CD at an extremely low cost, imagine the usual activities of a person from the moment he/her is born until dies only fit on a CD. The European Union, realizing the increasing technological progress, implemented various laws for the protection of personal data and human freedom, so after several laws, it ended up creating the GDPR which is automatically applied to all member states of the European Union as well as in third countries where personal data of European citizens are processed. The GDPR is opt-in / opt-out in relation to other personal data protection laws such as for example the CCPA which applies in California and is only opt-out, this is something very important and reinforces the effectiveness of the GDPR as it limits the use of personal data, but unfortunately there is not always European citizen's consent.

Keywords: GDPR; GDPR violation; Surveillance; Monitoring; E-mail; Networks; Security; Snoopy device; Privacy; European union

Introduction

GDPR is here to stay, it is a law that protects the privacy of European citizens, it assumes the consent of citizens to collect and process their personal data and of course it gives citizens the right to withdraw their consent whenever they wish. Unfortunately, not everything is so beautiful and harmonious, as there are methods of collecting citizens' personal data without, of course, asking for their consent, nor for the collection, not even for the processing of their personal data, of course, citizens cannot proceed with a complaint of deletion of their personal data as there is no evidence for the collection and processing of their personal data. One might ask, how is this possible? since the privacy policy is clear and not even for the processing of their personal data, of course, European citizens cannot proceed with a complaint of deletion of their personal data as there is no evidence for the collection and processing of their personal data. One might ask, how does it become innocent? since the aporito policy is clear and understandable, the answer has two [1] aspects, [2] the privacy policy is often written in simple and understandable language, but it contains statements which have a different interpretation for the citizens and a different legal meaning, [1] the lawful interception of information :for "good purposes": is not included in the privacy policy and nowhere it completely contradicts the GDPR and the private freedoms of

European citizens. The present research will focus more on the most widespread means of communication that exists today and of course that is e-mail. This research will highlight two [1] methods of interception, collection, and processing of personal data, of course presenting a diagram for further understanding of the problem that few people know exist.

Analysis

When the GDPR regulation was established, many rested believing that European legislation protects, and puts a brake on the collection and processing of personal data, but they did not think that the European citizen is not in a position to decide and know what is really happening. Cyber security and GDPR have a direct correlation, as now a day more than 90% of personal data is collected and processed carried out electronically, Both the collection and the processing must be carried out in secure information systems with recorded procedures. The security of both collected and processed information must be taken for granted, as it requires encrypted databases, encryption of sensitive information, prohibition of unauthorized access, secure information systems, and secure telecommunications networks [3]. Of course, to be able to secure an infrastructure to meet the conditions of collection and processing of personal data, should know very well how telecommunication systems work, should know encryption, network security, application security, and information systems security. Of course, all the above may be used in reverse, someone who is an expert in all of the above can be used to extract, intercept, store, and analyze personal data of citizens who communicate electronically, in this case in an e-mail account. An e-mail account is sure to contain personal data, as email today is necessary for the use of smart phones, as it is also a field for entering it into several public documents. An e-mail account may contain content with personal data, such as:

- First and last name.
- Contact numbers.
- Sensitive personal data.
- Bank information.
- Photos – short videos.
- Possible passwords.
- Corporate information that may contain personal data.
- Business activities.
- Metadata.
- Other personal identification data of the citizen.

Every citizen, especially the European citizen where it is directly related to the GDPR, by reading the privacy policy of the e-mail providers, believes and understands the following:

- User data remains in the European area.
- Content is encrypted.
- Will never have unauthorized access to an e-mail account.
- The process of collecting and using personal data
- The security implemented for the integrity and confidentiality of the information.

By reading the above, a citizen assumes and rests that the e-mail account that is created and used is a service to which only that citizen has access. Of course, the following cannot be written in the terms of use and privacy policy [4].

- The country's participation in transnational information exchange programs.
- The participation of internet service providers in information exchange programs.
- An e-mail account is encrypted for external users not for internal users.
- Who has access to the encryption / decryption keys.
- Location services recorded without user consent.
- The IP address.
- The history of visits that keep the Internet service providers.
- E-mail has no borders; each country applies different methods of collecting and processing information.
- The access of the secret services to collect and process information.
- The way of storing in a data center, the way of processing, searching and correlating the information.

Before presenting the 2 most effective methods of intercepting information from e-mail accounts, including personal data, it is useful to mention below, all the countries participating in the exchange of information, also known as the 14 Eyes Alliance: The participating countries are following:

- Australia.
- Canada.
- New Zealand.
- United Kingdom.
- United States.
- Denmark.
- Netherlands.
- France.
- Norway.
- Germany.
- Belgium.
- Spain.
- Sweden.
- Italy.

Do you see any European countries in the above list? Think again if there is real ownership and protection of personal data. Information does not follow the shortest route to its destination but the most advantageous route. This reference is made to understand that an information originating from the European Union is not strange in order to reach its schedule to pass through telecommunication networks of third countries with unforeseen consequences for the systems of other countries to collect personal data and process it without consent. How do they conduct the interception of information from e-mail accounts for "legal data interception"?

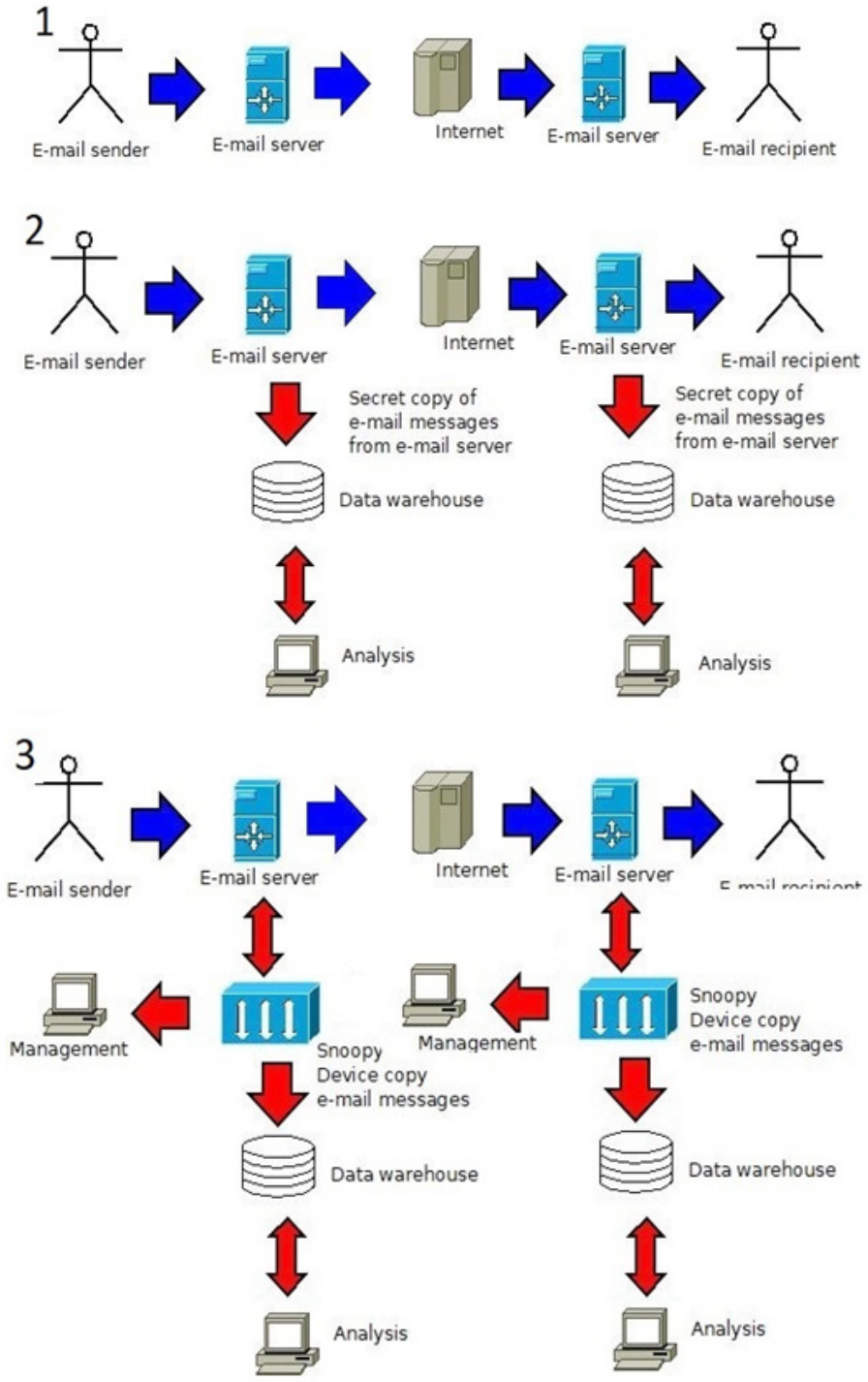

Figure 1.1:

In Figure 1, the 2 most important ones are presented. As we can see in the picture, the user after connecting to the e-mail account starts receiving and sending electronic mail, it is depicted in Figure 1 with the number 1. It is the unsuspecting citizen who makes use of the service believing that sends and receives electronic mails with other entities and that these mails are protected as only the e-mail account owner has access to his account. In Figure 1 in case 2, after the user logs in to the e-mail account and starts sending and receiving e-mail, the mail server is configured to share hidden copies of both incoming and outgoing mail to third-party data centers. storage and processing, without the citizen realizing anything of course. In Figure 1 in case 3, after the user logs in to the e-mail account and starts sending and receiving e-mail, in the infrastructure of the e-mail service provider, or the internet service provider, there is a device installed, which accepts commands remotely, it is able to intercept both incoming and outgoing e-mail content and transfer it to a data center for storage and processing, without the citizen noticing anything [4]. This device is called "Snoopy Device" (Figure 1).

E-mail systems are the target of personal data collection, for the following reasons:

- No access to personal data, so anyone who has access to the data center may have access to personal data.
- The citizens do not know where the data is stored and if encrypted and how.
- Metadata analysis.
- No citizen consent is given.
- Nobody knows the actual level of security they provide against attacks from viruses and external attacks and the security of the files that remain there.
- Nobody knows the actual privacy policies that were implemented.
- The legislation on security and personal data differs from country to country (outside the EU).

Conclusion

According to what was presented in this research, we conclude that the GDPR is not applied in the vast world of the internet, as the internet has no borders, and information can be transferred to third countries without knowing if there are transparent laws in these countries and, in general, if there is any personal data protection legislation applies. This research also re-examines the need to improve and continuously adapt the GDPR regulations so that it always adapts to current situations and always keeps pace with technological development. Finally, the legislation must become stricter and more specific with the collection-storage-processing-analysis of information, from information and personal data carried out in the context of transnational information exchange.

Acknowledgment

None.

Conflict of Interest

No conflict of interest.

References

1. Stephen Massey (2020) Ultimate GDPR Practitioner Guide (2nd Edition): Demystifying Privacy & Data. Fox Red Risk; 2nd edition.
2. Glenn Greenwald (2015) No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State. Picador; Reprint edition.
3. Christos Beretas (2018) Security and Privacy in Data Networks. Research in Medical & Engineering Sciences.
4. Christos Beretas (2018) Internet of Things and Privacy. Journal of Industrial Engineering and Safety.
5. Christos Beretas (2020) How Really Secure is TOR and the Privacy it Offers. Nanotechnology and Advanced Material Science.
6. Christos Beretas (2020) Cyber Hybrid Warfare: Asymmetric threat. Journal of Nanotechnology and Advanced Material Science.

Appendix

1	**GDPR**	General Data Protection Regulation
2	**CCPA**	California Consumer Privacy Act
3	**SNOOPY DEVICE**	Networking device who installed in ISP / mail servers to collect information, accept commands remotely