

**Online security and anonymity**

**Matteo Gianvenuti**

Summary

[Introduction 3](#_Toc185866080)

[What identifies you online? 3](#_Toc185866081)

[Alternatives that protect you (from simple to complex) 3](#_Toc185866082)

[Virtual Private Network (VPN) 3](#_Toc185866083)

[Proxy server 3](#_Toc185866084)

[The Onion Router (Tor) 4](#_Toc185866085)

[Operative System (OS) 4](#_Toc185866086)

[Whonix 4](#_Toc185866087)

[Conclusion 4](#_Toc185866088)

[Bibliography 5](#_Toc185866089)

# Introduction

The private companies, the organizations and the government aim to collect as much information about you as possible—just like in all the precious years, of course. Now and in the future, this will be much easier. This is because everything is going digital, mainly through hardware devices and software applications that do not pursue the user’s interest. They are not designed to protect your data, block the tracking attempts, anonymize, or protect your identity; on the contrary, they do the opposite.

As immediate consequence, the problem of personal safety and so anonymity (especially online) nowadays is greater than ever, and it will continue to grow. Those who controls the information of an individual have the full control over them. In a world like this democracy no longer exists. There can be no opposition in a system where people are completely controlled.

For these reasons, in this course thesis, we will attempt to set up a secure workstation by analyzing the security of various privacy-focused technologies, such as VPNs, Tor, Whonix.

# What identifies you online?

* **IP address:** The IP address serves two main functions: network interface identification and location addressing. It allows the packets delivery from the source host to the destination host on the internet (also in a private network) then it uniquely identify you. This mean the online activity is linked to the IP address and from it to a person or at least to a device. The IP address is typically assigned by the internet provider (more properly the internet access provider or the Internet Service Provider also known as ISP).

According to Italian laws, the ISP have to collect lots of information on the users, like: Information about who communicated with whom (e.g., IP addresses, connection timestamps, and duration). The internet access logs (the data must be retained for 12 months, extendable in case of a “crime”) and much more.[[1]](#one)[[2]](#two)[[3]](#three)[[4]](#four)

* **Browser and browser fingerprint:**
* **Cookies:**
* **Cross-site tracking and data aggregation:**
* **General tracking:**
* **OS and device information:**
* **Extra considerations, metadata:** The internet provider in almost all countries collect information on you eg Italy maintain all visited domains for months

# Alternatives that protect you (from simple to complex)

## Virtual Private Network (VPN)

## Proxy server

## The Onion Router (Tor)

## Operative System (OS)

## Whonix

# Conclusion

I

# Bibliography

[1] D.Lgs. 109/2008: <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1607282>.

[2] D.Lgs. 196/2003: <https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2003-06-30;196>.

[3] GDPR: <https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32016R0679>.

[4] Law 167/2017: <https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2017;167>.

[5]

[6]