Security and privacy considerations in autonomous agents

While innovative autonomous agents, making use of Artificial Intelligence (AI), have transformed accessing and leveraging of data, a broad range of applications need to be revisited to mitigate their impact.

Published on March 14, 2019



© Copyright: Shutterstock

Tagged with

* [Data protection](https://www.enisa.europa.eu/search?Subject%3Alist=Data%20protection)

Autonomous agents range from smartphones applications to autonomous robots supporting the supply chain in product development, for example; a key aspect in this regard is the data collected, mainly to support functionalities in a qualitative and timely manner.

Depending on the level of autonomy and context of operations, security and privacy considerations may vary. This ENISA study outlines AI technology used in autonomous agents in various application domains. It discusses the main security and privacy considerations and delivers a set of recommendations for relevant stakeholders and policy makers.

This study highlights relevant considerations, such as unauthorized autonomous systems, hijacking and misuse transparency and accountability, pervasiveness, retention and opacity of processing.

This study concludes with a set of recommendations, aimed at further influencing future EU policy initiatives, such as to:

* Further promote and support the adoption of security and ‘privacy by design’ principles as a pre-requisite during the inception, design and implementation of autonomous agents and systems;
* Develop a collaborative approach on the identification and the exchange of best practices. Gradually such initiatives should put forward sets of baseline security requirements;
* Endorse and support existing initiatives on the promotion and protection of human rights, through the establishment of appropriate ethical conditions related to autonomous agents;
* Establish a relevant framework for policy development, emerging technologies and new application areas.