OSINT – Legal research risk

OsintItalia
ASSOCIAZIONE di PROMOZIONE SOCIALE

Alessia Gianaroli

Mirko LAPI

CYBER CHALLENGE.IT

CYBERSECURITY NATIONAL LABORATORY

https://cybersecnatlab.it

License & Disclaimer

License Information

Disclaimer

- We disclaim any warranties or representations as to the accuracy or completeness of this material.
- Materials are provided “as is” without warranty of any kind, either express or implied, including without limitation, warranties of merchantability, fitness for a particular purpose, and non-infringement.
- Under no circumstances shall we be liable for any loss, damage, liability or expense incurred or suffered which is claimed to have resulted from use of this material.

Pay attention

Who performs Osint activities is not a hacker and does not violate the law

RISK

Any individual carrying out information gathering activities for any purpose, however lawful, is in any case potentially exposed to the risk of committing crimes

Personal Data

- Identification data
- Sensitive data
- Judicial data

The treatment of personal data 1/2

The GDPR defines the term personal data processing as any operation performed - manually or by electronic means - on the personal data of an individual

The treatment of personal data 2/2

by way of example: privacy code, art. 4, paragraph 1, letter a) concerns individual personal data, with regard to: collection, storage, processing, modification, linking and comparison, communication and diffusion to third parties, cancellation and destruction

It follows that the collection of information on individual is for all intents and purposes a treatment, while it is not intended for legal entity.

https://www.altalex.com/documents/codici-altalex/2014/02/10/codice-della-privacy

Information collection risks 1/3

Whoever carries out information gathering may be abusing the profession of private investigator (Art. 348 CP, cf. Art. 327-bis CPP)

Information collection risks 2/3

Some typical private investigator activities

static control activities

dynamic control activities

sound and video documentation

the use of satellite tracking devices (GPS)

camouflage or cover

Information collection risks 3/3

Similar to camouflage is the acquisition of information from the profile of a person on social media (e.g. Linkedin and Facebook) by accessing the platform with a fake profile

For example, asking for a contact by posing as another person, typically an acquaintance

Risk mitigation

To avoid the risk of practicing as a private researcher is essential to refrain from accessing social media using a false profile, especially if it is purported to be deceptive

Risk mitigation

In order to retrieve all information made publicly available on a social media site, it is preferable:

- carry out the consultation by not accessing the social network in question, for example by using a search engine as an intermediary
- use a profile that can be explicitly traced back to the person carrying out the search, also by activating the anonymous consultation mode

Thank you for your attention

OsintItalia
ASSOCIAZIONE di PROMOZIONE SOCIALE

Alessia Gianaroli

Mirko LAPI

CYBER CHALLENGE.IT

CYBERSECURITY NATIONAL LABORATORY

https://cybersecnatlab.it