European Journal of Social Sciences Studies
ISSN: 2501-8590
ISSN-L: 2501-8590
Available on-line at: www.oapub.org/soc

doi: 10.5281/zenodo.3877668 Volume 5 | Issue 3 | 2020

INVESTIGATIVE TECHNIQUES IN THE DIGITAL AGE: CYBERCRIME AND CRIMINAL PROFILING

Fulvio Greco[1]
Gianpiero Greco[2i]
[1]JD, LLM
Ministry of the Interior,
Department of Public Security, State Police,
Taranto, Italy
[2]PhD, MSc,
Ministry of the Interior,
Department of Public Security, State Police,
Milan, Italy
orcid.org/0000-0002-5023-3721

Abstract:
The advent of the Internet and social networks has reduced human and empathic relationships, consequently increasing virtual ones. Cyberspace offers the possibility of carrying out illegal acts with the perception of remaining unpunished. In this article we discussed the differences between crime and cybercrime which takes different forms within cyberspace such as cyberstalking, cyberbullying, online sexual offences and property crimes such as white-collar crimes. Furthermore, the evolution of criminal profiling in the digital age has been described and the profile of the cyber-criminal has been defined as outlined by the Italian State Police. The multiplication of criminal activities perpetrated through the web has led the Legislator to wonder about the most effective repressive methods to repress and try to ward off the numerous dangers that are wandering within cyberspace. The Italian legislator, through various legislative interventions, has introduced changes to the Penal Code as in article 612-bis, introducing in paragraph 2 an increase in punishment for the case in which the crime is committed through IT tools such as e-mail, SMS, chat malware and, above all, social networks. Also, the legislator included article 612-ter in the Penal Code to prosecute the illegal dissemination of sexually explicit images and videos. Finally, criminological research must consider that cybercrime has different variables than traditional crime and the evaluation of criminal behaviour should take into account the influence of the virtual dimension on the cognitive processes of the subjects.

Keywords: cyberspace; cyberviolence; criminology; cyberbullying; cyberstalking

[i] Correspondence: email gianpierogreco.phd@yahoo.com

1. Introduction to cybercrime

The technological evolution, with the increasing use of the Internet and social networks, has changed the concepts of "proximity", "communication" and "anonymity", and has reduced human and empathic relationships, consequently increasing virtual ones. *Cyberspace* is still an unknown place and we can say that we know and use only a small part of it. It is a complex ecosystem: if used correctly and controlled, it allows you to produce and exchange information remotely and is a great resource, not only for those who use the Internet for business purposes but also as a mere means of communication and exchange of opinions (Dodge & Kitchin, 2001). Through the network, users have the opportunity to get in touch with people who live on the other side of the globe without spending energy, quickly and without costs; if used correctly and lawfully, the Internet is an inexhaustible source of information. Cyberspace, however, also offers the possibility of carrying out, not infrequently, illegal acts, with the perception of remaining unpunished: the screen, in addition to acting as a filter between the agent and the potential victim of crime, allows the first to act undisturbed wherever you are, without the need to be physically on the crime scene (Barak, 2008; Nykodym, Taylor, & Vilela, 2005).

One of the substantial differences between traditionally understood crime and cybercrime is the fact that cybercriminals do not need to be physically on the crime scene (Clough, 2010). Through a simple program inserted within the organizational network and activated at any time, the offender will be able to carry out his criminal design undisturbed (Nykodym et al., 2005). Attempts have been made to indicate illegal conduct implemented through the use of IT or telematics devices; however, the most used term is *"cybercrime"*. Cybercrime means the "*offence in which the conduct or material object of the crime is related to an IT or telematic system, or perpetrated using such a system or hitting it*" (Cadoppi, Canestrari, Manna, & Papa, 2019). Cybercrime takes different forms within Cyberspace (Martellozzo & Jane, 2017). First of all, we find *cyberstalking*, defined as the digital transposition of the crime of persecutory acts referred to in article 612-bis of the Italian Penal Code.

Cyberbullying, an extension of the broader phenomenon called "bullying", consists in any form of pressure, aggression, harassment, blackmail, insult, denigration, defamation, identity theft, alteration, illegal acquisition, manipulation, illegal treatment of personal data in damage to minors, carried out electronically; as well as the dissemination of online content - also concerning one or more members of the family of the minor - whose intentional and predominant purpose is to isolate a minor or a group of minors, engaging in serious abuse, a harmful attack, or their ridicule.

Remaining on the topic of crimes against the person, we find crimes such as *sexting*, *online grooming*, *revenge porn*, and the crime of *sex extorsion* (Nicola & Powell, 2016). The Internet is also fertile ground for those wishing to commit property crimes. Some examples of these illegal activities are fraud, theft, money laundering and illegal trafficking, in which organized crime has its roots, however modifying its modus operandi, through the transition from the real world to Cyberspace. As far as the

economic-financial sector is concerned, cybercrime concerns the so-called *"white-collar crimes"* (Sutherland, 1987). White-collar crime is the expression used by Sutherland (1987) to indicate economic crime, with particular attention to the offenders and their position in the social and productive structure to which they belong. Among the typologies, the criminologist lists the following: "*forgery of company financial statements, stock exchange agiotage, direct or indirect corruption of public officials to secure advantageous contracts and decisions, false advertising, fraud in the exercise of trade, embezzlement and misappropriation of funds, tax fraud, misconduct in failure and bankruptcy*" (Sutherland, Merzagora, & Ceretti, 1986). The multiplication of criminal activities perpetrated through the web has led our Legislator to wonder about the most effective repressive methods to repress or, at the very least, try to ward off the numerous dangers that are wandering within Cyberspace. In this regard, it should be recalled that, with Law n. 547 of 23 December 1993 and Law n. 48 of 18 March 2008, which ratifies and implements the Budapest Convention on Cybercrime of the Council of Europe in our legal system, the Legislator has provided for stricter criminal sanctions, providing for rules relating to specific sectors and introducing and/or amending the regulations contained in the Criminal Code.

2. Criminal profiling in the digital age

Criminal profiling can be defined as the study of the delinquent psyche. It is a set of psychological techniques that serve to identify the offender based on the nature of the offence itself, as well as on the offender's modus operandi. In the technological era, it is not possible to draw up a criminological profile of an offender - property or against the person - which describes, in addition to the psychology of the offender, the possible scenarios and common conduct between categories of criminals, as well as his build or even the clothing worn during the crime. New technologies have made it possible to create a virtual world where the criminal has no face, has no emotions or feelings.

The first approaches inherent in the creation of a psychological profile of the criminals who act on the net were made towards those who commit crimes against the person. In this regard, it is noted, first of all, how the criminological evaluation of the offender's conduct must necessarily deal with technological progress and its influence on the cognitive processes of the agent. The Italian State Police attempted to outline the profile of the cyber-criminal, identifying him as "*a non-violent subject, with a low need to contain anxiety, determined by the fact that the crime does not take place in a physical place, strictly contact with the victim, but in the digital environment*" (Lorusso, 2011). This allows the subject to develop a lesser tendency to self-perceive himself as a true criminal.

Criminal profiling can be divided into two different models: inductive and deductive. Inductive profiling is based on the generalization of behavioural models from a statistical analysis of the data of convicted prisoners. It is based on inductive logic and discusses from the particular to the general. The inductive method uses the information of inmates contained within the databases to predict the personality traits and behaviour of the offender in the specific case (Petherick & Turvey, 2012). The deductive model, on the other hand, is based on deductive logic and discusses from the general to the

particular. Attention is based on the specific case: the evidence of the case is analysed and then used to build the behavioural profile related to the concrete case (Turvey, 1999). Regardless of the method used, the criminal profiling investigation technique rarely identifies the specific aggressor. Indeed, it accurately reduces the number of potential suspects and allows you to use the usually limited amount of investigative resources more effectively and efficiently (Douglas, Ressler, Burgess, & Hartman, 1986).

3. Criminal profiling applied to crimes against the person

Cyberstalking is the digital transposition of the crime of persecutory acts referred to in article 612-bis of the Penal Code, the criminal relevance of which was recognized by the Italian Legislator only in 2013 (Legislative Decree 93/2013, then converted by Law 15 October 2013, n. 119), making changes to article 612-bis of the Penal Code with the introduction, in paragraph 2, of an increase in punishment for the case in which the crime is committed through IT tools such as, for example, e-mail, SMS, chat malware and, above all, social networks. Psychology has developed, over time, different classifications of behavioural profiles of the stalker, in order to provide the competent authorities (law enforcement, criminologists, etc.) with the tools useful to efficiently deal with the phenomenon of stalking. In this regard, psychology identifies the following profiles:

1) The resentful is that person who tries to avenge the abandonment of the partner with repeated persecutory conduct; anger prompts him to attempt to destroy the victim's life;
2) The needy of affection is a profile of stalker who tries to establish a friendly relationship with the victim, up to the actual dependence. It is a kind of stalking that is most commonly found in patient-doctor relationships;
3) The incompetent suitor is a subject who can hide among work colleagues or university colleagues and who begins to court the victim with mere attention until he becomes persistent, generating in the latter a state of annoyance;
4) The rejected turns out to be such as a result of a refusal by the ex-partner or a suitor, persistently trying to create a bond with the victim - albeit negative - and preferring a similar relationship rather than the dissolution of the same;
5) Finally, the predator is one of the most violent subjects. In this case, the stalker's desire is sexual only; he is a planner and a hunter.

One of the differences found between stalking and cyberstalking is that, in the first case, the attacker, to persecute the victim, will have to follow him, lurk under the house or work and, therefore, limit the persecution over time. The cyberstalker, on the other hand, has the possibility of "torturing" his victim night and day, without having to get up from his chair but with the only help of an IT or telematic system. In this regard, an attempt was made to draw up a first behavioural profile of this subject: it seems that the conduct of the cyberstalker develops on the net by sending innumerable quantities of e-mails with offensive and demeaning tones, anonymous disclosure on the web of private material relating to the victim, the assumption of the victim's identity for malicious purposes and the intrusion into his computer system (Ziccardi & Perri, 2017, pp. 270-275).

Although it may seem reductive, this is a prime example of criminal profiling on a cybercriminal.

Cyberbullying, unlike traditional bullying, uses the net to express offences, threats within Cyberspace, using "*photos and video-shocks, e-mails and threatening instant messages in the chat, persistent SMS and MMS, websites and blogs, often violating the Civil Code or the Penal Code*" (Flamminio, 2009). What characterizes cybercrimes is the lack of empathy, physical and real contact with the victim. Compared to traditional bullying, electronic bullying completely cancels the space and distances between people, as well as the emotional dimension. In this regard, Faliva (2011) argues that the subject who is on the other side of the screen is perceived as an individual without body and emotions. The victim is not perceived as a "human being" and any feeling of empathy or identification is excluded. The types of attack on the net are manifold: by way of example, some of these categories will be listed below: in particular, the bash board is defined as a "message centre" within which to post offences and threats aimed at victims of the cyberbully. Trolling, on the other hand, is the "*dissemination of false information about the victim to collect the responses of other unaware subjects that can subsequently be used to persecute the victim*" (Fabrizio, 2015). The outing is the online sharing of embarrassing secrets and images of the victim (Gallina, 2009), while flaming consists in the dissemination of vulgar and violent messages within Cyberspace, to provoke real verbal battles.

Online grooming: with the development of new technologies, the crime of grooming, which consists of solicitation of minors for sexual purposes by an adult, has become established in the current criminological context. Specifically, the paedophile attracts the victim by trying to create a confidential and trusting relationship with her, to induce the latter to meet the attacker. Also, in this case, an attempt has been made to create a sort of profile of the paedophile who acts on the web: first of all, it can be seen how the groomer acts mainly on social networks - a channel now used globally - through the use of false profiles, designed and created specifically on the person you want to bait. In addition to creating a likely credible profile, the paedophile fills the victim with attention, adding "like" to each photo posted by the minor. As is known, among young people what matters is no longer just the appreciation that you receive in-person and, therefore, in real life but how popular and loved you are in social media. Once "the theatre has been basted", the groomer will begin to contact the victim in chat and, having gained his trust, will start an exchange of photos and videos with a sexual background. What matters most is that the attacker acts unconsciously on the victim; the children constantly ask themselves questions about sex but, for a sort of social taboo, they don't ask for explanations from their parents or professors - authoritarian and reference figures -. As a result, they will never reveal to the family that they are making such speeches with a stranger, especially if encouraged by the attacker not to say anything, with phrases such as "it is our little secret".

Revenge porn: it is a real "online revenge" and consists in the dissemination and sharing on the web of multimedia material with a sexual background, portraying ex-boyfriends or ex-girlfriends, to take revenge. Given the growing increase in the phenomenon and the need for reference legislation, the Criminal Cassation, Section V,

sentence of 16 January 2015 n. 6785, first included the phenomenon of revenge porn within the broader crime of defamation, referred to in article 595 of the Penal Code. The term itself indicates an act of revenge against the ex-partner at the end of a romantic relationship; this revenge consists in the disclosure and subsequent sharing of intimate material and sexual background (Ziccardi & Perri, 2017, pp. 279-282). After, through article 10, paragraph 1 of Law n. 69 of 19 July 2019, the new Article 612-ter was included in the Penal Code, which reads "illegal dissemination of sexually explicit images and videos" and is intended to punish anyone who publishes on the Internet, without the express consent of the persons concerned, private images or videos, however, acquired or held, made in intimate circumstances and containing sexually explicit images, with the consequent dissemination of sensitive data, with the intent to cause moral damage to the person concerned.

Sex extortion: the phenomenon of sex extortion has developed parallel to the use of the Internet. In particular, it is attributable to a series of behaviours designed to entice a potential victim "through the use of instant messaging, circumventing her to the point of inducing to carry out explicit sexual acts, at a distance, to extort money from her" (Ziccardi & Perri, 2017, pp. 282-285). Once again, an attempt was made to draw up a profile - at least about the "how" and "when" - to know and contrast the phenomenon. It is noted, first of all, that the modus operandi is almost always the same:

1) The first contact between attacker and victim occurs on social networks, where the two individuals begin to exchange general information about their passions, hobbies and jobs;
2) Subsequently, the conversations between the two subjects move on sexual themes. The attacker must earn the victim's trust who, otherwise, would never go so far as to send sexual material (photos, videos);
3) Once the attacker has gained full confidence from the victim, he goes from simple chat conversation, with the exchange of sexual material, to the video call. It is clear how, at this stage, the victim will go even further, with equivocal and increasingly sexual behaviours. The attacker will record and save everything, to have as much material as possible;
4) The last phase is blackmail: the extortionist makes known to the victim that he has recorded and saved all the material he sent himself. The blackmail consists of undermining the victim's reputation by convincing her that, if she does not pay a certain amount of money, the material collected by the attacker will be shared with the victim's friends, family, employers and partner.

It is curious to note how, while in the past the criminal's psychological and criminological profile was drawn up on his person, in the digital age the profile dedicated to sex extortion is elaborated on the "user profile" of the aggressor, to understand if it is real or it is a "fake". In particular, it is noted that there are elements that can inform the potential victim about the truthfulness or otherwise of the user profile that contacts her. To this end, the guidelines indicated by Ziccardi and Perri (2017, pp. 282-285) will be reported below:

a) The request for friendship on socials occurs without the two having had any contact in the real world;
b) The user profile appears recently created;
c) The contacts already present within the profile have no apparent geographical connection and the number of the same is limited;
d) The quality of the images inside the profile is high, which seems strange for a classic user profile;
e) The material present is discrepant;
f) The first contact between extortionist and a potential victim is direct and too conciliatory for two people who don't know each other;
g) Conversations are quickly conveyed by the attacker from simple speeches about work, hobbies and family to sexual topics.

5. Conclusions

In summary, the Italian legislator, through various legislative interventions, has introduced changes to the Penal Code to increase in punishment for the case in which the crime is committed through IT tools and to prosecute the illegal dissemination of sexually explicit images and videos. Furthermore, through the analysis of the literature, it has been shown that the criminological evaluation of criminal behaviour cannot fail to take into consideration the influence of the virtual dimension on the cognitive processes of the subjects. Cybercrime presents variables other than traditional crime, which seem to require particular and constant attention in the field of criminological research.

References

Barak, A. (2008). *Psychological Aspects of Cyberspace*. Cambridge: Cambridge University Press.

Cadoppi, A., Canestrari, S., Manna, A., & Papa, M. (2019). *Cybercrime*. Vicenza: UTET Giuridica.

Clough, J. (2010). *Principles of Cybercrime*. Cambridge.

Dodge, M., Kitchin, R. (2001). *Mapping Cyberspace*. London: Routledge.

Douglas, J. E., Ressler, R. K., Burgess, A. W., & Hartman, C. R. (1986). Criminal profiling from crime scene analysis. *Behavioral Sciences & the Law, 4*(4), 401-421.

Fabrizio, L. (2015). Le nuove forme della devianza. *Psicologia & Giustizia, 16*(1).

Faliva, C. (Ed.). (2011). *Tra normalità e rischio. Manuale di psicologia dello sviluppo e dell'adolescenza* (Vol. 65). Maggioli Editore.

Flamminio, L. (2009). *Tecnologia-mentis. Pedagogia e tecnologie nella TASCA*. Milano: Franco Angeli.

Gallina, M. A. (Ed.). (2009). *Dentro il bullismo. Contributi e proposte socio-educative per la scuola: Contributi e proposte socio-educative per la scuola.* Milano: Franco Angeli.

Law n. 48 of 18 March 2008. Retrieved from https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2008-03-18;48!vig=

Law n. 547 of 23 December 1993. Retrieved from https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:Legge:1993-12-23;547

Law n. 69 of 19 July 2019. Retrieved from https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2019;69

Legislative Decree 93/2013, converted by Law 15 October 2013, n. 119. Retrieved from https://www.altalex.com/documents/leggi/2014/02/26/femminicidio-conversione-in-legge-con-modificazioni-del-d-l-n-93-2013

Lorusso, P. (2011). *L'insicurezza dell'era digitale. Tra cybercrimes e nuove frontiere dell'investigazione*. Milano: Franco Angeli.

Martellozzo, E., & Jane, E. A. (2017). *Cybercrime and Its Victims*. London: Routledge.

Nicola, H., & Powell, A. (2016). Sexual Violence in the Digital Age: The Scope and Limits of Criminal Law. *Social & legal studies, 25*(4), 397-418.

Nykodym, N., Taylor, R., & Vilela, J. (2005). Criminal profiling and insider cybercrime. *Digital Investigation 2*, 261-267.

Penal Code. Retrieved from https://www.brocardi.it/codice-penale/

Petherick, W. A., & Turvey, B. E. (2012). Criminal Profiling: Science, Logic, and Cognition. In *Criminal Profiling* (pp. 41-65). Elsevier.

Sutherland, E. H., Merzagora, I., & Ceretti, A. (1986). *La criminalità dei colletti bianchi e altri scritti*. Unicopli.

Sutherland, E. H. (1987). *Il crimine dei colletti bianchi.* Milano: Giuffrè.

Turvey, B. (1999). *Criminal profiling: An introduction to behavioral evidence analysis*. New York: Academic Press.

Ziccardi, G. & Perri, P. (2017). *Tecnologia e diritto*. Milano: Giuffrè.