Chapter 17
Cyber-Crimes against Adolescents:
Bridges between a Psychological and a Design Approach

Filipa da Silva Pereira
University of Minho, Portugal

Marlene Alexandra Veloso de Matos
University of Minho, Portugal

Álvaro Miguel do Céu Gramaxo Oliveira Sampaio
Polytechnic Institute of Cávado and Ave, Portugal

ABSTRACT

At young ages there is an increase in reports of intimidation, harassment, intrusion, fear, and violence experienced through Information Technologies (IT). Hacking, spamming, identity theft, child pornography, cyber bullying, and cyber stalking are just few examples of cyber-crimes. This chapter aims to contribute, from a psychological and design perspective, to an integrative viewpoint about this complex field of cyber-crime. In this chapter, the most common types of cyber-crimes, epidemiological data, and the profiles of cyber victims and aggressors' are approached. The studies that identify the factors contributing to IT misuse and to growing online vulnerability, principally in adolescents, are also discussed. Likewise, the central explanatory theories for the online victimization and the risk factors for victimization and perpetration online are addressed. Finally, some cyber-crime prevention strategies are anticipated, in particular among young people, seeking to provide clues to the consolidation of recent policies, namely at the digital design level.

INTRODUCTION

During the last 15th years, the Internet and the other ITs have radically transformed the world, mainly in terms of communication and social interaction. In areas such as science, education, health, public administration, commerce and the development of the global net, the Internet offers an unmatched variety

DOI: 10.4018/978-1-5225-0808-3.ch017

of benefits. Therefore, information technologies turn out to be a communication tool deep rooted in the quotidian of world population. This applies especially to youths who present high indices of utilization and digital skills (Haddon, Livingstone & EU Kids Online network, 2012; Madden, Lenhart, Cortesi, Gasser, Duggan, Smith & Beaton, 2013). In this way, it is not surprising, as IT imposes as a mean of mass communication, the increase in reports of harm, intimidation, harassment and violence experienced through IT: experiences commonly known as cyber-crime (Dempsey, Sulkowsk, Dempsey & Storch, 2011).

Cyber-crime is a concept that integrates a set of activities related to the use of telecommunications networks for criminal purposes (Kraemer-Mbula, Tang & Rush, 2013) and it is described in the Portuguese law nº 109/2009 of 15th of September. It can comprises a diversity of (1) anti-social activities, such as those supported by computers (e.g., sending spam, malware) and (2) offenses aimed at a specific target (e.g., cyber stalking, cyber bullying) (Kim, Jeong, Kim & So, 2011). To accomplish cyber-crime activities, there are a variety of manipulation techniques (e.g., bribe, threat) and different ways through which Internet users can find themselves involved in risk behaviors (e.g., contact with strangers, the sharing of personal information) (Whittle, Hamilton-Giachritsis, Beech & Collings, 2013). However, the Portuguese penal code only contemplates as cyber-crime, anti-social activities supported by computer (material damages of technical content). In contrast to what happens in the United States, for example, cyber stalking or cyber bulling is not criminalized in the Portuguese law as a criminal offense, being only possible to criminalize individual actions that make up this form of persistent persecution and harassment (e.g., threats, identity theft and invasion of privacy).

The Internet turned into a space in which the more traditional crimes may take new forms and prosper in a totally immaterial environment (Clarke, 2004). The criminal activities that previously required the physical presence of his actors, in a place and specific time, are now possible independently of the physical location or time (Reyns, 2013). Because of this, the mysticism that surrounds the cyberspace and the anonymous nature of Internet means that individuals with reduced likelihood to start a criminal act in the real context (e.g., children and adolescents) can easily began to have a high probability to do so in the online context (McGrath & Casey, 2002).

As acknowledged previously, with the diffusion of IT, there is a tendency for cyber-crime to increase, both in its frequency as in the sophistication of the acts and techniques to commit it. However, it is not possible to eradicate this side of the online world. Thus, the solution is to investigate those new forms of cyber aggression in order to understand, control and minimize potential forms of cybernetic victimization and their impact (physical, mental and social health loss) (Marinos et al., 2011).

Despite cyber-crime being looked at with a growing scientific interest, this has not been sufficiently reflected from the psychological approach, which may have an important role in understanding the key factors that allow an early identification of features and enables the prediction of the course and evolution of these behaviors.

Cyber-crime is substantially different from traditional crimes, since it benefits from the timelessness, the possibility of anonymity and the absence of a restricted space (Yar, 2005). There are several theories that have been developing explanations about cyber-crime, including the routine activity theory (Cohen & Felson, 1979), the general theory of crime (Gottfredson & Hirschi, 1990) and the social learning theory (Skinner & Fream, 1997).

After exploring the cyber victims and aggressors' profiles, we address the main contributions of the above-mentioned theories for the understanding of the data related to cyber aggressors and cyber victims. The recognition of the steps implicated on cyber-crime and the conditions that facilitate it, permits allows the development of preventive actions towards cyber-crime (Clarke, 2004).