The Consent of the Victim as Legal Defence in Cybercrime cases

Maxim DOBRINOIU[*]

Abstract

The rise of Cybercrimes provides with great concerns among users, industry, banking sector or public institutions in terms of how much secure their computer systems or computer data are. Both Ethical and Non-Ethical hacking came-up as viable solutions for any natural or legal person willing to perform its own security checks. Taking into consideration the nature of such security evaluation techniques, that in certain situations may be regarded as cybercrimes, there should be a proper understanding of the circumstances when the victim may grant permission to the attackers to perform specific tasks against its own systems or data, especially when these belongs to a public institution.

Keywords: *cybercrime, Ethical Hacking, criminal law, consent, computer system, legal defence*

1. Introduction

Considering the scary statistics about the real level of Cyber-related crimes and offences in the nowadays modern and technological society we live in, and the dark forecast provided by the Cybersecurity researchers, more and more individuals and organisations are keen on taking precautions and perform various tests and scans of their own computer systems in order to evaluate the risk of becoming a Cybercrime victim, with all known consequences: stolen virtual or real identity, stolen or damaged data, financial or even property loss, privacy disturbance, affected business or current activities, information leakage and so on.

To prevent this happening, both individuals and legal persons are in pursuit for the best solutions available on the market to assess their cyber vulnerabilities, ranging from simple AV protection to complex hacking-style techniques.

But, asking professionals from both Ethical and Non-Ethical hacking communities or IT security companies to perform such complex penetration tests or vulnerability scans means to accept your computer systems being hacked, personal of financial data being compromised (even temporarily), IT infrastructure being affected (for a while) or remotely controlled by others. In other words, there are some risks that the willing natural or legal person should take on when deciding to let a hacker or an external IT security specialist to perform hacking-style tasks on your systems.

Knowing that their hacking-type actions may be regarded as computer crimes, the Ethical Hackers or the IT security professionals are taking precautions and choose to conclude specific commercial/civil contracts with the clients, while seeking for a legal approval for their further activities against clients' computer systems or computer data.

This means that even if they technically commit a cyber-related crime (e.g. hacking, access to a computer system, data or system interference, data interception, data transfer or alteration), every such act may be considered *per se* as "authorized", "legal" or "with right", and thus they are exempted from being charged or prosecuted for committing a crime (according to the law).

While in the case of a natural person (individual) the situation is clear and a valid approval given represents the legal ground for the other party (the "attacker") to not be prosecuted, things are a little bit complicated in the case of a legal person, as it will be detailed below.

2. Doctrine views on Consent as Legal Defence

In the Romanian Criminal Code, the "consent of the victim" is regarded as a clause that justifies the commitment of a crime. The legal provision states that "*it is justified the act described by the law when committed with the consent of the injured party, if the party could legally dispose of the affected or endangered social value*"[1].

In the same time, the same provision states that "*the consent of the injured person does not produce any legal result in case of crimes against life, as well as in the situations when the law itself excludes the justifiable effect*".

Most of the authors agree that, with any occasion the law does not explicitly forbid, the owner or the holder of the social value (ex. computer system, computer data etc.) may accept any threat, risk, damage or prejudice to that value, considering that the act by which the value was endangered or affected in any way

* Associate Professor, Faculty of Law, "Nicolae Titulescu" University of Bucharest (email: **office@e-crime.ro**).

[1] Article 22 align. 1 of the Romanian Criminal Code

is legal, authorized or with right (*volenti et consentienti non fit injuria*)[2].

In Cyberspace this justification clause operates only based on the following conditions:

The consent should be granted only by the owner or the legal holder of the further affected value. So, there is a need to prove the link between the consenter and the computer systems or the computer data that may be endangered by the hacking-type evaluation techniques.

Another condition is that the consent regards a value/good the consenter has a legal right to dispose of. This way, we may consider just a few situations when the consent is valid and justifies a possible cyber-related crime.

Things are more clear and simple when the person authorizing the hacking is the real owner of the affected value and has the legal ability to dispose of his own values (ex. computer system, computer data).

The scenario becomes more complicated when the values protected by the law belongs to the state – through the patrimony of a public institution/authority.

According to many authors, if the values targeted by the perpetrator's actions are bound to so-called *collective rights* (such as national security, state authority, public trust, public safety, family etc.), these values cannot be protected by the justifiable clause (legal defence) of consent.

While the owner of the goods can transfer to a third party the right to alter of affect in any way its own goods (including computer systems and data), the public institution – acting as the administrator of the state goods and interests - has certain limitations in what regards the capacity of disposal of those goods in such manner.

But the more important aspect of this analysis resides in the primary condition for the existence of consent, as an accepted legal defence: the existence of a crime. Unless a crime occurs, there is no need for a justification, chiefly not for a consent.

Based on an opinion[3] we should agree with, if the lack of consent is one of the main conditions for a certain activity to legally be considered a crime, therefore the existence of such a consent (whether is a permission, authorization, provision of a law or a contract) places the respective activity out of the criminal code provisions, due to the missing typicality requested by the principles of criminal law.

3. The legal characteristics of the Cyber-related crimes

The Cyber-related crimes have all got a specific condition: to be committed "without right". In this respect, it is worth mentioning that the Romanian legislator took over the Council of Europe Convention on Cybercrime's provisions and also considered that "without right" means: a) that the perpetrator has no authorization based on a law or a contract, b) even if an authorization exists, the perpetrator exceeds its limits, or c) the perpetrator has no permission – from the individual or legal person competent, according to the law, to grant it - to use, administer, control a computer system or to undergo any scientific research or to perform any other operation in a computer system.

As envisaged by the CoE Convention, the Romanian legislation also took into consideration the necessity to criminalize the intentional and unlawful behaviour of a person regarding a computer system or computer data.

Moreover, the CoE Convention, in its Explanatory Report, stated that the "without right" provision reflects the insight that the conduct itself may be legal or justified "not only in cases where classical legal defences are applicable, like consent, self-defence or necessity, but where other principles or interests lead to the exclusion of criminal liability"[4].

So, basically, the term "without right" is set forward to cover any other situation (scenario) where the hacking activity is not performed in the general framework of legal defences, excuses, justifications or undertaken based on a formal authorization, whether legislative, executive, administrative, contractual or consensual.

In other words, if the cyber-related activity is "with right", there should be no crime and no criminal liability for the eventual Ethical Hacker.

The "right" to perform any actions against computer systems or data relies on the ability of the person which either owns or just administers (control) the target system or data. And, while the owner has a commonly recognized and legal right to do whatever act against his goods and values, not the same regime may apply in case of a public institution, where the manager has the responsibility to preserve and to protect the safety of the goods and values he administers or possesses.

4. Conclusion

As revealed by the above analysis, in the Ethical Hacking scenarios (hacking with consent), there is a legal problem posed by the existence of an authorization for the performance of specific cyber-attacks and hacking techniques against computer systems and data, while these computer systems and data belongs to the state.

Considering the theory of the consent, as a legal defence mentioned by the Criminal Code, the authorization issued by the management of a public institution for cyber-attacks is a condition for not claiming the existence of any computer-related crime,

[2] Vasile Dobrinoiu, Ilie Pascu and co-authors, *New Criminal Code commented. General Part*, Universul Juridic Publishing House, 2016, page 185.
[3] C. Mitrache, C. Mitrache, *Romanian Criminal Law, general part*, Universul Juridic Publishing House, 2014, page 189
[4] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce5b – point 38

but, in the mean time, the question remains to what extent the management of the respective public institution indeed has the right to issue such authorization for the performance of specific computer-related activities, by a third party, against the computer systems and data that are covered by a national interest.

While there should be a right for the public institution manager to issue an authorization/permission for the performance of certain hacking-type activities in order to identify the vulnerabilities related to the state-owned computer systems and data he has a legal obligation to protect and secure, certain limits and restrictions may also be considered in this respect, as the protection of the state interests and values needs a broad approach, from both legal perspective and cyber-security concerns.

Therefore, a possible solution may be for the management of a public institution to allow only certain specific hacking techniques to be applied or used by the pen-testers. The kind of techniques that do not harm, interfere or affect in any way the good functioning of the systems or the confidentiality, integrity and availability of the data stored or processed by the target systems.

In this way, the need for cyber-security will meet the other legal aspects related to the right of disposition (of the public institution manager) and the permission to be granted to the IT security specialists to perform their tasks with the confidence that no crime is committed and no law is trespassed.

References:

- Council of Europe Convention on Cybercrime, available at: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf
- Explanatory Report on the Convention on Cybercrime, available at:https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce5b
- http://www.cybercrimelaw.net