CRIMINAL LIABILITY IN THE CASE OF VENDORS OF SOFTWARE AND HARDWARE FURTHER USED IN CYBERCRIME ACTIVITIES

Maxim DOBRINOIU*

Abstract

In the recent years have been noticed an ascending trend in commercialization of spyware products, either for lawful government use in combatting crimes or national security threats, or for people interested in their own electronic protection or monitoring others placed under their care or legal responsibility.

While the use of this kind of wiretapping devices and programs may be legitimate under the criminal procedural laws, for example in collecting electronic evidence, digital investigations or prosecuting crimes, the illegal situations are often linked to the violations of human rights, crimes against confidentiality, integrity and availability of data and systems, infringing privacy and data protection, infringing intellectual property rights, data breaches, frauds, domestic violence, intimate partner abuse, and many more. Most of the legislations simply address the criminal liability of the final user of such devices or applications, which appear to be clear enough based on the final results of their illicit behavior, but the vendors seem to be let outside the criminal law or placed in a grey zone of legal interpretation.

Taking into consideration the scope of spyware devices and programs that results in various forms of direct or indirect (personal) abuse of another, it is important to assess the legal impact of this kind products in both social and economic relations and how the marketing of such items contributes to the further commission of crimes.

The paper thus aims at identifying the possible legal implications for the individuals and companies that deal with producing, adapting, selling, distributing or making available software applications, computer programs, scripts or hardware devices and equipment that may further be used unlawfully, without right, for infringing human rights or for performing cyber-attacks against people, businesses, administration or ICT infrastructures of any kind, and finding the best suitable legal reasons that sustain a possible criminal liability of the creators/vendors.

Keywords: *criminal liability, illegal operations, criminal law, cybercrime, spyware, mobile surveillance*.

1. The context of computer programs and devices being used for surveillance

What do names like Pegasus[1], Candiru[2], FinFisher[3], Galileo[4], mSpy, PhoneSherrif[5]and FlexiSPY, Spyera Qustodio, SpyBubble, TheWiSpy, Spyic, FamiSafe, Cocospy, MobileSpy.at, uMobix, eyeZy, Hoverwatch, XNSPY, pcTattletale, Minspy, Spyier, MobiStealth, iSpyoo have in common? They are parts of a large worldwide business enterprise dealing with producing and distributing software and hardware for eavesdropping, monitoring, data interception, wiretapping and generally all kind of electronic surveillance.

The clients? Mostly governments, either democratic or so-called dictatorial. But, also, ordinary citizens (employers, frustrated employees, teachers, students, parents of minors, legal guardians of minors or disabled people, work colleagues, intimate partners, etc.), driven by nefarious thoughts or willing to protect themselves or their family members from the online threats.

These products are often sold as for serving the law (in the destination countries), for law enforcement and national security purposes mainly. Yet, recently, strong allegations showed up and even decent proofs about such products being used for fulfilling other objectives, mainly linked with the infringing (digital) rights and unlawful surveillance of different individuals (politicians, businessmen, journalists, human rights activists etc.).

"Spyware" has been defined by the US Trade Commission as "software that aids in gathering information about a person or organization without their knowledge and that may send such information to another entity without the consumer's consent, or that asserts control over a computer without the consumer's knowledge"[6].

* Associate Professor, PhD, Faculty of Law, "Nicolae Titulescu" University of Bucharest (e-mail: maxim.dobrinoiu@univnt.ro).

[1] Notorious spyware program created by the Israeli company NSO Group from Tel Aviv, being responsible for infecting and eavesdropping mobile phone (iPhone or Android) belonging to politicians, human rights activists or journalists from more than 45 countries.

[2] Surveillance software designed for Windows OS, developed by an Israeli company with the same name.

[3] Surveillance software developed and commercialized by UK-German company Gamma International.

[4] Spyware software developed by Hacking Team company.

[5] Spyware software developed by the US company called Retina X Studios LLC.

[6] https://www.ftc.gov/sites/default/files/documents/reports/spyware-workshop-monitoring-software-your-personal-computer-spyware-adware-and-other-software-report/050307spywarerpt.pdf.

Although the definition is too general, we may exclude the situations when a code/program/script is collecting information about a user, but in the form of firmware or software updates, usage of devices (ex. Internet of Things), online behavior on websites (ex. cookies) or even social or commercial platforms (where a certain level of user consent is necessary).

Documenting the products (both software and hardware), one could notice the disclaimer the selling companies are making visible to anybody that may question the legality and legitimacy of the whole process of producing such applications and devices to the selling, distributing or making available to the interested persons.

In the vast majority of the cases, these companies claim that their products help governments and security services to fight against violent crimes, organized crime, terrorism and threats to national security. In the absence of relevant official statistics provided by governments or law enforcement agencies, we may suppose that this is true and such digital surveillance products really do the job they were created for.

For all that, no one may ascertain for sure that SW and HW designed for the surveillance of the terrorists or organized crime members are not sold, distributed or made available in any form to private entities or interested (and financially powered) individuals.

We have to recognize that this kind of software and devices fill a gap where security services or law enforcement agencies are defeated by the cutting-edge technologies and strong encryption facilities now terrorists or organized crime members are using. Simply, (cyber) criminals and terrorists have better technology for encrypting than investigators have to decrypt them[7].

Authors say that commercial spyware has grown into an industry estimated to be worth twelve million dollars, while it is largely unregulated and increasingly controversial[8].

Technically, irrespective the product is a keylogger, a trojan or a Remote Access Tool (RAT), they have almost the same features and provide specific services of accessing a device or a computer system, intercepting and reading computer data (emails, chats), capturing relevant data (usernames, passwords, card and account details, screenshots), eavesdropping the calls, tracking terminal GPS location, exfiltrating data, remotely switch on the device's microphone, monitoring the target's activity on social networks, recording the user's internet browsing history and much more.

Depending on their complexity, these surveillance products are installed in the target device (computer system, smartphone, tablet, PDA etc.) usually through Phishing attacks, other Social Engineering tactics, tools and procedures (TTP), "0-day" vulnerabilities or by exploiting human misconduct or lack of security "hygiene" related to the use of electronic devices or Internet.

There are many reasons one would like to buy, use and control such spy-enabled devices or computer programs, ranging from legitimate ones, such as tracking a stolen or lost smartphone, monitoring a child or a disabled relative or even tracking the incoming and outgoing calls or messages[9] and up to illegal ones, such as spying on a business partner, a wife, a girlfriend or a neighbor, a competitor, a boss or a designated target person (a journalist, a human rights activist, a political opponent and so).

The number of worldwide customers varies from ten-thousands to millions[10]. And the prices range from tens of euro (US dollars) to thousands (per month, if with subscription), depending on the features, stealth and capabilities.

There are public insights that various governments facilitated this spyware industry big revenue over time, in some cases even offering permissions (license) for chosen vendors to sell their surveillance products abroad, despite indicators of further possible human rights violations or other personal abuses.

Most of such products are advertised on publicly available commercial platforms, online markets, mobile stores, security forums, while some of them are imported, distributed, sold or made available in covert ways (but not necessarily out of the law), through closed commercial links, usually involving government agencies, prosecutor's office, police forces or security services.

2. Legal provisions on illegal operations with computer data, applications and devices as acts of commerce

Based on the legal provisions of the Council of Europe "Budapest" Cybercrime Convention of 2001[11], most of the European (and even non-European) countries created, modified, or updated their own criminal laws including different crimes against

[7] https://www.nytimes.com/2022/01/28/magazine/nso-group-israel-spyware.html.

[8] See Ronan Farrow, *How Democracies Spy on their Citizens*, The New Yorker, 18 April 2022, available at https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens (accessed on 02.05.2022).

[9] https://www.softwaretestinghelp.com/phone-spying-apps/.

[10] mSpy product is reportedly as having nearly 2 million active customers.

[11] Available at https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561.

confidentiality and integrity of data and computer systems, with specific references to the illegal operations with computer data, applications and devices.

Under art. 6 – misuse of devices, the CoE Convention on Cybercrime urged states "to adopt such legislative and other measures to establish as criminal offence, when committed intentionally and without right:

a) the production, sale, procurement for use, import, distribution or otherwise making available:

- a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5;
- a computer password, access code or similar data by which the whole or any part of a computer system is capable of being accessed"[12].

This proposal of a distinct legal provision criminalizing the misuse of devices and programs has further been adopted in the substantive criminal law of many countries, such as: Austria (Section 126c of the Criminal Code), Belgium (art. 259bis, art. 314bis, art. 550bis, art. 550ter of the Criminal Code), Bulgaria (art. 319e of the Criminal Code), Canada (art. 190(1) and art. 342.2 of the Criminal Code), Estonia (art. 216^1 and art. 284 of the Criminal Code), France (art. 323-3-1 of the Criminal Code), Germany (art. 202c of the Criminal Code), Finland (chapter 34, sections 9a and 9b of the Criminal Code, and sections 6 and 42 of the Data Protection Law), Hungary (art, 300/C and art. 300/E of the Criminal Code), Lithuania (art. 198-2 of the Criminal Code), Portugal (art. 3 and art. 6 of the Law no. 109/2009 on the Cybercrime), Romania (art. 365 of the Criminal Code), Spain (art. 400 and art. 536 on cybercrime of the Criminal Code), and United States of America (18 US Code, art. 2512 on the manufacturing, distribution, possession, and advertising of wire, oral, or electronic communication intercepting devices prohibited).

Other legislations seem to be even stricter in dealing with interception or electronic surveillance devices and programs, for example the Canada Criminal Code and the New Zealand Crimes Act of 1961 (part 9A), that specifically mention that "possessing" (CA), "selling" (CA, NZ), supplying (NZ) or even "purchasing[13]" (CA) of interception devices is an offence[14], thus placing *ab initio* the commercial conduct as a crime.

Moreover, the Section 216D(1) of the same law makes it an offence "to offer for sale or supply or to offer or invite or agree to sell or supply to any person an interception device unless this is done for a lawful purpose as described in Section 216D(2)"[15].

More or less, almost all the above legal provisions have certain features in common, such as:

- the reference to products like: computer programs, applications, computer data, devices etc.;
- the products are either prohibited *de jure*, or their use may be unlawful, without right, without a legitimate reason etc.;
- the products are described as being designed, made, created, produced, manufactured, adapted etc. as for being used in a sort of specific operations, like communication intercepting[16] (US), committing an offence or a crime[17] (FR), infringement of the secrecy of telecommunications[18] (AU), to introduce a set of executable instructions…. to produce any of the non-authorized actions[19] (PT), which allow to get access to a computer system with the intention of committing crimes[20] (EE);
- the principal behavior prohibited by the law consists of specific verbs like produce, supply, distribute, make available, possess, detain, obtain (for use), offer (for sale), dispose of, introduce, sell, import, make accessible, manufacture, advertise, hold for commercial purposes etc. referring mostly to legitimate commercially-related operations;

In some of the national legal provisions, the commercial conduct represents an offence simply if committed *intentionally*, *without right*, *without legitimate reason* etc., but in other legislations, the commercial operations with such devices and programs constitute an offence only when put together with the real intention of the offender (ex. *knowing that the device has been used or is intended to be used to commit a crime*[21]), that is creating a computer system or a computer data-related harm to the victim. Other states preferred to join the two aspects of illicit conduct with (or misuse of) devices and programs, namely the

[12] Art. 6, CoE Convention on Cybercrime (ETS no. 185) available at https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185 accessed on 26.04.2022.

[13] See art. 190 (1) of the Criminal Code of Canada, available at https://laws-lois.justice.gc.ca/eng/acts/c-46/page-28.html#docCont

[14] https://www.lawsociety.org.nz/news/lawtalk/issue-834/criminal-liability-for-mobile-phone-spying-in-nz/.

[15] *Ibidem*.

[16] See 18 U.S. Code chap. 2512, available at https://www.law.cornell.edu/uscode/text/18/2512, accessed on 26.04.2022.

[17] See art. 323-3-1 Code Penal Francais, available at https://www.legifrance.gouv.fr, accessed on 26.04.2022.

[18] See Section 126c of the Austrian Criminal Code, available at www.coe.int/cybercrime/documents, accessed on 26.04.2022.

[19] See art. 3, 6 and 7 on the Portugal Criminal Code, available at https://www.anacom.pt/render.jsp?contentId=985560, accessed on 26.04.2022.

[20] See art. 2161 of the Estonian Criminal Code, available at https://www.riigiteataja.ee/en/eli/522012015002/consolide, accessed on 26.04.2022.

[21] See art. 342.2 of the Criminal Code of Canada, available at https://laws-lois.justice.gc.ca/eng/acts/C-46/section-342.2.html.

"absence of permission" or "the absence of right" and the harmful bunch of actions against the victim.

We acknowledge that the vast majority of the legislations provide general indicators in describing the surveillance devices or programs (ex. *intercepting device* or *a device/computer program, designed or adapted primarily for the purpose of committing a crime* etc.), thus not offering a comprehensive definition that may cover all the situations from the real life.

For example, in such kind of broad definition, one could understand that a *packet sniffer* may fall under the prohibition of the law, whereas this device/computer program is in reality designed for helping internet service providers or network administrators to identify data traffic congestions, anomalies or to filter suspect or malicious content.

This is why, being so general, the legal provisions may be very restrictive in some occasions, while permissive in others, situation that could represent an advantage for interested persons.

The issue is very complicated due to the fact that spyware or other monitoring or surveillance devices or programs are of dual-use, meaning that they may be used for both legitimate and illegal purposes, and often only the unlawful behavior of the spyware operator could bring the legal question upon the vendor itself too.

3. The right of the seller vs. the rights of those being abused by the seller's products – possible criminal indictments

As we discovered studying a lot of commercially available surveillance products, most of the spying devices or computer programs are properly (and even carefully) advertised as helping people to protect themselves, their (electronic) property or their families (while online). Others simply claim that using the products may be legal if the target person expresses its consent for the monitoring.

It is true that on the market one can find different types of surveillance devices and programs, and depending on the legislation of the country the producer (vendor) is based, the products are commercialized in "full-feature" forms (more invasive) or in the "lite" ones (less intrusive).

There has also been observed that the vendors also make different statements on their commercial platforms, indicating that the products are capable of performing actions that may be intrusive (in the privacy of another) or regarded as illegal due to the power to facilitate an unlawful behavior of the client. It is obvious that such a disclaimer used by the vendor represents just a self-declaration of non-liability against the (criminal) law.

In other instances, researchers found that the vendors are using a "curated list of positive customer testimonies which outline how spyware provided succor to its users and solved relationship problems"[22].

Moreover, analyzing the marketing aspect round the spyware industry, one could also notice the index terms, such as "spyware", "tracking", "monitoring", "surveillance", "spouse monitoring", "employee tracking" etc., used by all the producers in order to manipulate the consciousness of the target customers, based on their internal intellectual desirability or mental predisposition, into determine them to purchase their products.

As we all see, there are numerous vendors that produce, import, distribute or make available, in any form, software applications or devices further used in (cyber) criminal activities, and thus, in doctrine as well as in judicial practice, the situation raised the question whether such a particular vendor should be or not indicted for participating in the commission of any of those (cyber-related) crimes.

App stores and web platforms that enable selling spyware programs to consumers also play a role as intermediaries that can facilitate the sales of stalkerware (surveillance/monitoring kits) through their platforms[23]. It was found that, "despite active efforts made by Apple and Google to enforce app developer policies and agreements against such apps, research shows evidence of a continued, albeit decreased, presence and availability of stalkerware on popular app stores"[24].

We continue[25] to state that, the vendor may have a criminal liability, because, acknowledging the technical details and characteristics of the software applications, computer programs or the electronic devices produced, imported, distributed or made publicly available – meaning that they could (or should) be used in cyber-related criminal activities, against

[22] D. Harkin, A. Molnar, E. Vowles, *The commodification of mobile phone surveillance: An analysis of the consumer spyware industry*, Crime, Media, Culture: An International Journal, 2019, available at https://journals.sagepub.com/doi/full/10.1177/1741659018820562 (accessed on 30.04.2022).

[23] See examples www.top10spyapps.com, www.cellspyapps.org, www.bestphonespy.com.

[24] C. Khoo, K. Robertson, R. Deibert, *Installing fear: A Canadian Legal and Policy Analysis of Using, Developing, and Selling Smartphone Spyware and Stalkerware Applications*, Citizen Lab Research Report no. 120, 2019, available on https://citizenlab.ca/2019/06/installing-fear-a-canadian-legal-and-policy-analysis-of-using-developing-and-selling-smartphone-spyware-and-stalkerware-applications/ (accessed on 30.04.2022).

[25] M. Dobrinoiu in V. Dobrinoiu and colab., *New Criminal Code Commented*, 3rd ed., Universul Juridic Publishing House, Bucharest, p. 908.

computer data and computer systems or against individuals – they have the intellectual capacity to pursuit, to foresee or to accept a criminal outcome.

Notwithstanding their initial legal disclaimer about the absence of liability, the vendors may not intend to determine someone to commit a crime while buying one of their monitoring products, but, in many cases, it was proven that they acted in a way of actually promoting the nefarious capabilities of such products, highlighting the privacy-intrusive features that changed the client's initial mental resolution (ex. to monitor his child online activity) to another mental resolution that resulted in a crime.

Analyzing the *modus operandi* in what regards the commercial behavior of the spyware vendors, researchers found that "the advertised level of data-monitoring is highly invasive, offering clear scope for disproportionate and abusive surveillance"[26] of individuals.

According to some other opinions, the vendors should not be held legally liable due to the absence of their guilt. And this may be the case of a knives or axes vendor which cannot be indicted for a manslaughter crime committed by one of his clients.

In all these particular scenarios from the objective reality, we notice that the law does not forbid the producing, the selling, the import or the distribution of any such items or tools (knives, axes, firearms, batons) that may be one day used in the commission of a violent offence.

We have to agree with other authors stating that "the surreptitious capabilities of the spyware program are what render the sale of the program illegal, even if it were theoretically possible that the program could be used in a manner that provides the individual user with a defense"[27].

Per a contrario, as CoE Convention on Cybercrime recommended (as from 2001) and many states already adapted their legislations accordingly, national legislators have chosen to criminalize, even slightly different, the commercial activities with devices or computer programs that may be used in the commission of (other) cyber-related crimes and various other offences.

Moreover, in reality, the subjective implication (*mens rea*) of the vendors (CEO, CIO, security staff, programmers etc.) of such surveillance products in the crimes further committed by their clients (most of them against the availability and confidentiality of computer data and systems) consists of intent, either a direct intent or an indirect intent. It is thus excluded the negligence.

All the scenarios and stories we detailed above, and many other incidents and cases from the judicial practice show that the creators/vendors produce many of such software applications or electronic devices with a dual final outcome: one legal – when the product is going to be used according to the laws of the nations where they are registered or the buyers are registered with, and also one illegal – when the product is designed to (help to) commit a crime, to infringe human rights, to unlawfully perform surveillance etc.

The criminal intent results from the creator/vendor's inner evaluation of the (real or eventual) illegal result of his actions, and the actual behavior or the creational/commercial-type activities that he further performs related to the spyware product, from the early stages of project, design, architecture, technical characteristics and features, capabilities enabled, functions to be provided and the presence or the lack of safeguards for the target (the individual whom the program would eventually be used against), and more important the marketing and advertising tactics meant for the "offer" to meet the (unlawful) "need".

Only this way, the "dual-use"-related defense of the vendor may be rejected as inadmissible, and his participation in the further commission of a crime with the use of his spyware product will have the meaning of criminal liability.

Criminal liability may also occur when the vendor fails to act under its legal duty (established by the criminal, civil, commercial legislation of a nation county), while he is proven as being reasonable able of doing this. But this means that there should be created new legal mechanisms (other than criminal law provisions) that may coerce or determine the companies to conduct their commercial activities in certain (ethic) ways, obligations that may be opposable to them.

4. Conclusions

Whether deployed entirely "legitimately" or illegally, spyware has the capacity to threaten persons and lives, while fueling corrosive relationships between parents and children, intimate partners, employees and employers, citizens and governments, in addition to the damage the spyware can provide when used against specific targets, such as activists, journalists, politicians or commercial actors.[28]

Although there are numerous legislations that criminalize (when intentional and without right) the making, producing, possessing, selling, offering (for

[26] D. Harkin, A. Molnar, E. Vowles, *op. cit*.
[27] C. Khoo, K. Robertson, R. Deibert, *op. cit*.
[28] See D. Harkin, A. Molnar, E. Vowles, *op. cit.*

use or for sale), purchasing, distributing or making available devices or computer programs that enable the commission of (mostly cyber-related) crimes or violations of privacy and human rights, just few cases were brought to the courts of justice.

Inexplicably, despite numerous reports in media and scientific researches about the unlawful trade and use of spyware programs or devices, there is a reluctancy from the judicial side in criminal investigating and prosecuting this kind of offence, with few exceptions[29].

In our conclusion, the creator or the vendor of spyware programs or devices may face criminal liability in all the legislations analyzed herewith, but only if it could be demonstrated that it has conducted its commercial activities in such a way that the spyware product was created, developed, advertised, distributed or sold with the intent to be used by the buying operator as a necessary and indispensable tool for the commission of a (computer-related) crime or an offence against life, physical or mental integrity, liberty, privacy, other human rights or general safety of another individual.

References

- Vasile Dobrinoiu and collaborators, *New Criminal Code Commented*, 3rd ed., Universul Juridic Publishing House, Bucharest, 2016;
- Diarmaid Harkin, Adam Molnar, Erica Vowles, *The commodification of mobile phone surveillance: An analysis of the consumer spyware industry*, Crime, Media, Culture: An International Journal, 2019, available at https://journals.sagepub.com/doi/full/10.1177/1741659018820562;
- Cynthia Khoo, Kate Robertson, Ron Deibert, *Installing Fear: A Canadian Legal and Policy Analysis of Using, Developing, and Selling Smartphone Spyware and Stalkerware Applications*, Citizen Lab Research Report no. 120, 2019, available on https://citizenlab.ca/2019/06/installing-fear-a-canadian-legal-and-policy-analysis-of-using-developing-and-selling-smartphone-spyware-and-stalkerware-applications/;
- Ronan Farrow, *How Democracies Spy on their Citizens*, The New Yorker, 18 April 2022, available at https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens;
- Lorenzo Franceschi-Bicchierai, Joseph Cox, *Inside the „stalkerware" surveillance market, where ordinary people tap on each other's phones*, Vice, 18 April 2017, available at https://www.vice.com/en/article/53vm7n/inside-stalkerware-surveillance-market-flexispy-retina-x;
- Kate Lyons, *Stalkers using bugging devices and spyware to monitor victims*, The Guardian, 13 February 2018, available at https://www.theguardian.com/uk-news/2018/feb/13/stalkers-using-bugging-devices-and-spyware-to-monitor-victims;
- https://www.justice.gov/opa/pr/man-pleads-guilty-selling-stealthgenie-spyware-app-and-ordered-pay-500000-fine;
- Criminal Code of Austria;
- Criminal Code of Belgium;
- Criminal Code of Bulgaria;
- Criminal Code of Canada;
- Criminal Code of Estonia;
- Criminal Code of France;
- Criminal Code of Finland;
- Criminal Code of Germany;
- Criminal Code of Hungary;
- Criminal Code of Lithuania;
- Criminal Code of New Zealand;
- Criminal Code of Portugal;
- Criminal Code of Romania;
- Criminal Code of Spain;
- Criminal Code of the United States of America.

[29] See Man Pleads Guilty for Selling 'StealthGenie' Spyware App and Ordered to Pay $500,000 Fine https://www.justice.gov/opa/pr/man-pleads-guilty-selling-stealthgenie-spyware-app-and-ordered-pay-500000-fine.