ENCRYPTION: DUALISM AND VULNERABILITIES

Isabela PORCIUS*

Abstract

Nowadays, people tend to enjoy living more and more in their parallel lives within the digital environment. But this phenomenon comes with its own challenges and responsibilities. The main challenge, which is also a responsibility, is to ensure cybersecurity.

Encryption represents one of the most commonly used information security measures, but, at the same time, a very debatable measure. Despite its vital role for ensuring cybersecurity, encryption also facilitates criminal activities in cyberspace and even cyberterrorism.

Therefore, I am going to present the two antagonistic ways in which encryption can be used, namely, cybersecurity and cybercrime, and their impact on the life of every person and on society as a whole. When analyzing the dual nature of using encryption, it is equally important to discuss the topic of encryption vulnerabilities, which undoubtedly generate data vulnerability. In this context, a lot of controversy has risen around the issue of State intervention through backdoors.

Key Words*: Encryption, cybersecurity, cybercrime, blockchain, backdoors*
JEL Classification: [K24]

1. Encryption dualism: from cybersecurity to cybercrime

It has been stated that *today, nearly all participants in society use encryption,* including State Governments, corporations, different organizations and also individuals (Saper 2013, p.677).

As a result, it becomes clear that, in nowadays society, which is sustained through the use of technology, States, different entities and citizens are generally trying to adapt to this reality, in order to fully benefit from the positive effects of applying technology. Technology cannot be compared to other existent facilities, given the fact that it has generated a genuine world revolution.

Encryption is regarded as being at the top of the hierarchy of cybersecurity mechanisms (Swire & Ahmad 2012, pp. 454-455). Contrary to the general opinion, that encryption is being used only to facilitate adequate communication and to protect stored information, encryption is actually used to achieve various purposes, including the security of electronic transactions (Swire & Ahmad 2012, p. 453).

* PhD. candidate, Faculty of Law, Babeş-Bolyai University, Cluj-Napoca, Romania.

Encryption has become fundamental to security on networks like the Internet, and it is used in every industry to securely store and transmit confidential data (Castro & Mcquinn 2016, p. 6). Moreover, it has been acknowledged that there is no substitute for encryption, as a security measure, when it comes to data in transit, data at rest and to authentication (Swire & Ahmad 2012, p. 457). As a conclusion, encryption is a defining component of cybersecurity, taking into consideration the fact that its efficiency in this domain is undoubtable.

In order to analyze the entire context of encryption within the sphere of cyberspace, it is important to take into consideration also the damaging facet of using encryption.

One of the problems identified by the relevant published literature is the possibility of every person to have online access to the source code of end-to-end encryption software, a situation which gives individuals and entities the possibility to adapt the software and even to create their own version of encryption software, which has been used also for conducting terrorism (Graham, 2016, pp. 22-23)[1]. The previous British Prime Minister, David Cameron, has insisted, after the attack which aimed the offices of the French magazine Charlie Hebdo, upon the fragility of public safety when confronted with end-to-end encryption, which denies the access of the crime investigation authorities (Bienkov, cited in Castro & Mcquinn; 2016; p. 11). The Director of the European Union Agency for Law Enforcement Cooperation (Europol) talked about encryption as being *the biggest problem* encountered in the fight against terrorism (Price, cited in Castro & Mcquinn 2016, p. 11).

On one side, it has been stated that, although encryption offers significant advantages for cybersecurity, it is also being used for committing cybercrime through the emerging phenomenon of *going dark*[2]*,* which disables the capacity of applying *traditional investigative techniques* and the capacity of applying specific methods of digital forensics, an emerging branch of forensic science[3]. On the other side, US case law has raised the issue of

[1] The article presents the case of Rajib Karim, a British Airways employee, who conspired with al-Qa'ida, between 2009 and 2010, in order to plan attacks against the British Airways and the US Airways; communication between Rajib Karim and al-Qa'ida was enabled by a complex encryption system.

[2] *Going dark* means using encryption mechanism for committing crime, *to communicate and store information, thus avoiding detection and incrimination.*- Graham; 2016; p.20. The term *going dark* has been used by FBI's former General Counsel Valerie Caproni, in the context of crime investigations being disabled by data encryption.- Valeria Caproni, *Going Dark: Lawful Electronic Surveillance in the Face of New Technologies,* Federal Bureau of Investigations, February 17,2011, https://www.fbi.gov/news/testimony/going-dark-lawfulelectronic-surveillance-in-the-face-of-new-technologies, *apud* Castro & Mcquinn; 2016; p. 7.

[3] European Union Agency for Law Enforcement Cooperation (EUROPOL)- European Cybercrime Centre (EC3), *INTERNET ORGANISED CRIME THREAT ASSESSMENT (IOCTA)*, 2017, p. 63.

whether or not obliging a suspect to decrypt files from his own devices could represent a breach of the right against self-incrimination.[4]

Nevertheless, it can be observed that, sometimes, the necessity of the authorities to fight against encryption mechanisms, in order to discover and to punish cybercrime, may come in antithesis with the rights of the individuals, more exactly the right to use cybersecurity measures and the right to privacy. In these situations, different forms of abuse may appear from the authorities involved.

A surprising, yet alarming case of abuse from authorities is the one which involved the National Security Agency from the United States of America. More exactly, the National Security Agency had modified, according to their interests and without informing the public, a cryptography standard that the National Institute of Standards and Technology (NIST) had issued in 2006 (Greenemeier, cited in Castro & Mcquinn 2016, p. 16).

It is clear that in many cases there is a continuous battle between law enforcement bodies and individuals. Therefore, all of the above mentioned aspects must not be neglected when it comes to determining the priority of the interest (whether public or private), when dealing in court with a particular case.

In conclusion, encryption has two sides, a positive side, which facilitates cybersecurity, and a negative side, which supports cybercrime. Unfortunately, these two sides coexist and they influence each other.

Furthermore, it has been said that in the case of encryption, we may talk about *a dual-use technology,* and the negative side of encryption is not *per se* a sufficient argument for States to prohibit the use of encryption*,* like cars are

[4] United States Court of Appeals for the Third Circuit, *U.S. v. Apple Macpro Computer*, 2017, no. 15-3537, viewed 14 April 2020, from: https://law.justia.com/cases/federal/appellate-courts/ca3/15-3537/15-3537-2017-03-20.html. While investigating a case of child pornography, the authorities executed a search warrant according to which the suspect had to give the passwords of the encryption software used on his devices. The suspect challenged the search warrant, considering that it had breached his right against self-incrimination. The court stated that, his allegation is not going to be taken into consideration, because the investigation authorities had demonstrated both the existence of the files with child pornography and the fact that the suspect had the possibility to access the encrypted files. This criteria was borrowed from *In re Grand Jury Subpoena Duces Tecum* Dated Mar. 25, 2011 (11th Cir. 2012), 1346-1349. In another case, the court gave the crime investigation authorities the permission to oblige a person to hand over the private encryption keys.- United States Court of Appeals for the Fourth Circuit*, In Re: Under Seal*, no. 13-4626, 2013, viewed 14 April 2020, from: https://cases.justia.com/federal/appellate-courts/ca4/13-4625 /26/0.pdf?ts=1381462357. The appellant was an e-mail service provider. Its customers benefited from both encryption applied before an e-mail was stored on the server and encryption used in the transit of communication between the e-mail servers and the customers. The second type of privacy protection, which used Secure Sockets Layer-that implied asymmetric encryption, was the one for which the appellant refused to hand over the encryption keys, having as argument the fact that the security of the communications carried out through its servers could be jeopardized.

not prohibited just because criminals can use them to escape justice. (Castro & Mcquinn 2016, p. 26).

In order to protect the rights and the interests of all the parties involved in the activities carried out in cybersociety, it is important to identify legal solutions which have the ability to place the positive side of encryption above the negative side. An example which supports this reasoning is the attitude of Europol, which has recommended, in the context of cybercrime, that Member States of the European Union should keep and also extend their commitment to Europol with respect to organizing campaigns for enhancing awareness and for improving prevention related to cybersecurity, where data encryption plays a vital role.[5] Moreover, the WannaCry Attack from May 2017 is considered as having as *an unintended positive aspect* a genuine phenomenon of *global awakening,* by *creating an opportunity for IT security issues to be taken more seriously by businesses and organisations.*[6] Unfortunately, it had been necessary to occur major damages (as a result of this attack) so that State authorities and their citizens finally understand that cyberspace has to be treated with responsibility, given the fact that it is a space full of opportunities both for the ones with good intentions and for the ones with harmful intentions.

2. The case of Bitcoin and blockchain

A particular topic, which is focused on the use of encryption, is Bitcoin, the virtual currency which nowadays is subject to controversy, given the fact that it is situated, from the legal point of view, in a *grey area* (Turpin 2014, p. 352). As a result of the mistrust of the way in which financial institutions exercise their role as payment processors in e-commerce, the distributed network related to Bitcoin was proposed as a saving solution, also because it offered anonymity in conducting transactions and absence of costs when processing payments (Nakamoto, cited in Turpin 2014, p. 338). Despite these facts, Bitcoin has an important position in the hierarchy of means that facilitate cybercrime, but, recently, strong competition has risen from other types of currency based on encryption, such as Monero, Ethereum and Zcash.[7]

The distributed network of stored transactions, known as blockchain, upon which is built also the Bitcoin system, could be used to improve cybersecurity, as a result of its *decentralized* (Lunn, cited in Shackelford & Myers 2016, p. 22) character (without an authority or a central control entity), which allows the cooperation of all the parties involved[8] and even the emergence of *polycentric*

[5] European Union Agency for Law Enforcement Cooperation (EUROPOL)- European Cybercrime Centre (EC3), *INTERNET ORGANISED CRIME THREAT ASSESSMENT (IOCTA)*, 2017, p. 16.
[6] *Idem*, p. 30.
[7] *Idem,* p. 13.
[8] Also regarding the validation of the perfomed transactions (Shackelford & Myers 2016, p. 43).

governance[9]. Furthermore, blockchain is useful for ensuring cybersecurity, also due to its *public ledger* role, which could be a solution for the problems and incidents that certification authorities are dealing with when they issue digital certificates (Shackelford & Myers 2016, pp. 26-27).

There are also other important ways in which blockchain can be used, such as for creating *smart contracts,* which have the ability of self executing, without any human intervention, or blockchain can even be used for establishing *smart property,* which includes assets that can be managed only on the Internet (Wright & De Filippi 2015, p. 1).

Smart contracts are based upon the idea that the binding force of a contract has its origin in conditional structures that can be transposed in computer programming (Raskin 2017, p. 312). As a result, although, apparently, Law and Computer Programming are languages situated at opposite poles, when it comes to smart contracts, the two languages join forces and generate a new instrument for transactions. In the category of *strong smart contracts* (which require substantial costs in order to be modified or terminated), an important issue is the lack of *post factum* control, because once these contracts are concluded, they have to be executed (Raskin 2017, pp. 310-311). Blockchain technology, due to the fact that it represents a distributed decentralized network, can take the role of courts in interpreting contractual clauses (Raskin 2017, pp. 316-317), and it can also take the role of the intermadiary who confirms the transaction (McKinlay, Pithouse, McGonagle & Sanders 2017, p. 9). Moreover, in this scenario, breach of contract is also prevented and the steps of contract execution have to be each taken into consideration, given the fact that by introducing them in blockchain, they can be verified by the users of the network (Raskin 2017, p. 319); information is added to the network only after obtaining the consent of all the users from the network regarding the validity of the operation and after this moment, the operation cannot be invalidated (Franco, cited in Wright & De Filippi 2015, p. 7).

As a result, smart contracts require only the agreement of the parties to conclude the contract, without subsequently being possible for turbulences to appear, from the inside or from the outside, in the process of executing the contract. It has been affirmed that smart contracts are one of the first technological achievements, after the printing press, that have definitely disturbed the legal activity (Wright & De Filippi 2015, p. 10). By adopting the use of smart contracts at large scale, people may have the possibility to issue an actual legal framework adapted to their own legal and technical needs (Wright & De Filippi 2015, p. 40).

[9] In such a context, the rules (laws) that have been applied (as a result of the agreement reached by all the parties involved) can be spontaneously adapted and improved (Shackelford & Myers 2016, pp. 34-35).

The uncertain legal regime of smart contracts has determined the suggestion to include in their content some clauses referring to dispute resolution, which will protect the consumers (McKinlay, Pithouse, McGonagle & Sanders 2017, p. 10).

If there are no efficient legal measures to guarantee the protection of the rights and interests of users, it is possible that the development of blockchain mechanisms will generate surveillance of the users, just as it was the case of the Internet, which is currently being used by States to monitor their citizens and by private entities to monitor and record the activity of users (Wright & De Filippi 2015, p. 53). As a result, although blockchain offers various solutions to facilitate activities conducted in cyberspace, it can also generate the restriction of the rights and liberties of the actors from cyberspace. Like encryption, blockchain also has a dual nature.

It has been affirmed that the development and the popularity of blockchain and of its various applications that are useful for the society, would generate a new Law branch named *"Lex Cryptographia"*, which would contain *a set of rules administered through self-executing smart contracts and decentralized (and potentially autonomous) organizations* (Wright & De Filippi 2015, p. 48).[10]

I consider as being not at all surprising the idea of creating a new Law branch to deal strictly with analyzing the implications of using encryption and with offering the proper legal solutions to the issues generated by the broad use of encryption, given the fact that Law has the responsibility to create a balance between its principles and its concepts, on one side, and the challenges of the present world in which we live in, on the other side.

3. Encryption vulnerabilities: Backdoors

It has been stated that, generally, all types of encryption are targeted by particular specialized attacks, such as *attacks assisted by a flaw known to the attacker or "backdoors"* (Swire & Ahmad 2012, pp. 429-430). Therefore, backdoors represent voluntary or involuntary interruptions of the encryption mechanism, which determine the occurrence of major vulnerabilities that can be exploited by cybercriminals when conducting cybercrime. Moreover, backdoors diminish the trust generated through using encryption.[11]

---

[10] Regarding the *decentralized organizations*, these represent an alternative, facilitated by blockchain, to the current business landscape. More exactly, businesses would function based on smart contracts, transactions would be registered and supervised in the blockchain, and the power of decision would not be held by central bodies, because it would be decentralized. The autonomous character refers to the fact that these entities do not need human intervention to function from the moment they are included in the blockchain (Wright & De Filippi 2015, pp. 15-17).

[11] High Level Group of Scientific Advisors, *Cybersecurity in the European Digital Single Market,* Scientific Advice Mechanism (SAM) Independent Scientific Advice for Policy Making, Scientific

Backdoors can be applied *either at algorithmic level or at implementation level*.[12]

The large public erroneously considers that States' Secret Services are successful in defeating any encryption mechanism (Graham 2016, p. 21). The truth is that an encryption mechanism which is precisely built, from the technical point of view, without errors, is not vulnerable (Graham 2016, p. 21).[13] When data is encrypted, the only available data is metadata, which means information regarding the sender and the receiver of the electronic communication, the period of time during which the communication was conducted and the amount of data transmitted (Castro & Mcquinn 2016, p. 14). Despite all these facts, States' Secret Services have, in some situations, the possibility to install backdoors without the targeted individual or the targeted entity being aware.[14]

In the context in which the Federal Bureau of Investigation (FBI) solicited the US legislative body to issue regulations concerning the obligation to establish backdoors, it has been affirmed that such regulations are going to reveal their futility, given the fact that they are not going to be applicable in the case of software products created in other States and also in the case of terrorism, where encryption mechanisms are developed based upon open-source software which is publicly available (Graham 2016, p. 25).

Again at the level of the United States of America, specialists from the area of information technology policy (Castro & Mcquinn 2016, p. 1) consider that central State authorities should not adopt measures that are going to restrain encryption mechanisms or that are going to diminish the effects of encryption mechanisms, because such measures would have as consequences the following: the decline of the security level for citizens without unlawful

---

Opinion No. 2/2017, opinion issued at the request of the European Commission, Bruxelles, p. 30, from: https://ec.europa.eu/research/sam/pdf/sam_cybersecurity_report.pdf#view =fit&pagemode =none.

[12] High Level Group of Scientific Advisors, *Cybersecurity in the European Digital Single Market,* Scientific Advice Mechanism (SAM) Independent Scientific Advice for Policy Making, Scientific Opinion No. 2/2017, opinion issued at the request of the European Commission, Bruxelles, p. 31.

[13] It was also affirmed that it could even be impossible to decrypt an encrypted message without the necessary key, when it is a case of *strong* encryption. - High Level Group of Scientific Advisors, *Cybersecurity in the European Digital Single Market,* Scientific Advice Mechanism (SAM) Independent Scientific Advice for Policy Making, Scientific Opinion No. 2/2017, opinion issued at the request of the European Commission, Bruxelles, p. 31.

[14] An example is the case of Juniper Networks, an enterprise specialized in technology, which, in 2015, has discovered that, during 3 years, its products have been compromised by backdoors included by the National Security Agency, as a result of modifying the cryptography security standard issued by the National Institute of Standards and Technology (NIST) (Zetter, cited in Castro & Mcquinn 2016, p. 17; Price, cited in Castro & Mcquinn 2016, p.17; Weinmann, cited in Castro & Mcquinn 2016, p. 17).

intentions and for businesses; the hindrance of the opportunities for American businesses to gain reputation at global level; the obstruction of the suitable development of information technology.

At the level of the European Parliament, it has been asserted that the use of end-to-end encryption should be promoted and, if there are technical possibilities, the use of end-to-end encryption should even be imposed, in order to establish proper conditions for network security and for the security of services; in the same context, it has been affirmed that Member States of the European Union should not have the possibility to impose obligations which would generate *the weakening* of security, such an obligation being the inclusion of backdoors.[15]

If State authorities would impose the inclusion of backdoors, this would be prejudicial to small businesses and manufacturers, because they would risk losing the trust of consumers, who would consider other options available on the market; it would not be the case of such issues for corporations, given the fact that most of the times they do not have competition. [16]

Despite the fact that authorities invoke, against the monopoly of the user over his own encryption keys, the possibility to have access to data based upon a warrant obtained from a judge, in the case of a search warrant issued for a private property, the authorities are not also entitled to have access to data which is well hidden, just as it is the case of *information that is buried in someone's backyard or memorized but never written down* (Castro & Mcquinn 2016, p. 23). This is a very useful practical reasoning presented by the relevant published literature in opposition to the demand of the authorities to have access to encrypted data.

---

[15] European Parliament, *Report on the proposal for a directive of the European Parliament and of the Council establishing the European Electronic Communications Code (EECC) (recast),* 19 October 2017, from: www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A8-2017-0318+0+DOC+PDF+V0//EN, Opinion of the Committee on Civil Liberties, Justice and Home Affairs for the Committee on Industry, Research and Energy, reporter: Morten Helveg Petersen, amendment no.9, pp.464-465. The same idea is presented in:- European Parliament, *Report on the proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)*, from:http://www.europarl.europa.eu /sides/getDoc.do?pubRef=/EP//NONSGML +REPORT+A8-2017-0324+0+DOC+PDF +V0//EN, Opinion of the Committee on the Internal Market and Consumer Protection for the Committee on Civil Liberties, Justice and Home Affairs, amendment no. 18, p. 162.

[16] High Level Group of Scientific Advisors, *Cybersecurity in the European Digital Single Market,* Scientific Advice Mechanism (SAM) Independent Scientific Advice for Policy Making, Scientific Opinion No. 2/2017, opinion issued at the request of the European Commission, Bruxelles, p. 32. Despite the fact that the cited source presents the negative effects of backdoors just from the point of view of small businesses, I consider that medium-sized businesses would have the same fate, because the trust of their customers is also fragile.

Regarding the argument of the authorities that access to encrypted data would help them in the fight against crime and even against terrorism, it has been affirmed that there are also other methods available for the authorities, through which they can discover, investigate and punish committed crimes, such as obtaining metadata and also other traditional investigation and forensic methods (Castro & Mcquinn 2016, p. 25).

Conclusions

Encryption is not just about Computer Programming. This level of comprehension has already been exceeded, as a result of the methods through which the features of encryption have been exploited.

Its various and complex applications offer many facilities for improving cybersociety as a common good, this representing the positive side of using encryption. As an indispensable cybersecurity measure, encryption raises the trust of users regarding technological facilities. Moreover, through blockchain, encryption also provides mankind a lot of opportunities to develop.

But, at the same time, there are many interests involved in cyberspace, and some of these interests seek only their fulfillment (a private good which is damaging for others), regardless of the rights and needs of the ones that do not have power to decide (as it is the case of proposals for introducing backdoors) or regardless of the needs of the ones that do not have unlawful intentions and become victims (like cybercrime); this represents the negative side of using encryption.

Unfortunately, this vicious circle continues to exist until encryption is going to be properly understood, approached and regulated.

Bibliography

1. Castro Daniel & Mcquinn Alan, (2016), *Unlocking Encryption: Information Security and the Rule of Law*, Information Technology & Innovation Foundation, March, viewed 13 April 2020, from:http://www2.itif.org/2016-unlocking-encryption.pdf.
2. Graham Robert, (2016), "How terrorists use encryption", *CTC SENTINEL* (Combating Terrorism Center at West Point), 9 (6), June, viewed 14 April 2020, from: https://ctc.usma.edu /app/uploads/2016/06/CTC-SENTINEL_Vol9Iss614.pdf.
3. McKinlay John, Pithouse Duncan, McGonagle John & Sanders Jessica, 2017, "Blockchain: background, challenges and legal issues", *DLA Piper*, viewed 14 April 2020, from:https://www.dlapiper.com/~/media/Files/Insights/Publications/2017/06/Blockchain_background_challenges_legal_issues_V6.pdf.
4. Raskin Max, (2017), "The Law and Legality of Smart Contracts", *1 Georgetown Law Technology Review* 305, viewed 14 April 2020, from: https://ssrn.com /abstract=2959166.
5. Saper Nathan, (2013), "International Cryptography Regulation and the Global Information Economy", 11 *Nw. J. Tech. & Intell. Prop*. 673, viewed 13 April 2020, from: https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?referer=https://www.bing.com/&httpsredir=1&article=1205&context=njtip.

6. Shackelford Scott & Myers Steven, (2017), "Block-by-Block: Leveraging the Power of Blockchain Technology to Build Trust and Promote Cyber Peace", Yale Journal of Law and Technology (2017 Forthcoming); *Kelley School of Business Research Paper* No. 16-85, viewed 15 April 2020, from: https://ssrn.com/ abstract=2874090.
7. Swire Peter & Ahmad Kenesa, (2012), "Encryption and Globalization", *Columbia Science and Technology Law Review*, 13, viewed 13 April 2020, from SSRN: https://ssrn.com/abstract=1960602> or <http://dx.doi.org/10.2139/ssrn.1960602.
8. Wright Aaron, De Filippi Primavera, (2015), *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*, viewed 15 April 2020, from: https://ssrn.com/ abstract=2580664.
9. Turpin Jonathan B., (2014), "Bitcoin: The Economic Case for a Global, Virtual Currency Operating in an Unexplored Legal Framework", *Indiana Journal of Global Legal Studies*, 21(1), viewed 13 April 2020, from: http://www.repository. law.indiana.edu /cgi/viewcontent.cgi?article=1557 &context=ijgls.

International Documents and Court Cases

1. European Parliament, Report on the proposal for a directive of the European Parliament and of the Council establishing the European Electronic Communications Code (EECC) (recast), 19 October 2017, from: www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML +REPORT +A8-2017-0318+0+DOC+PDF+V0//EN.
2. European Parliament, Report on the proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), from: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+ REPORT +A8-2017-0324+0+DOC+PDF+V0//EN.
3. European Union Agency for Law Enforcement Cooperation (EUROPOL)-European Cybercrime Centre (EC3), INTERNET ORGANISED CRIME THREAT ASSESSMENT (IOCTA), 2017, High Level Group of Scientific Advisors, Cybersecurity in the European Digital Single Market, Scientific Advice Mechanism (SAM) Independent Scientific Advice for Policy Making, Scientific Opinion No. 2/2017, opinion issued at the request of the European Commission, Bruxelles, from: https://ec.europa.eu/research/sam/pdf/sam_cybersecurity_report.pdf#view=fit& pagemode=none.
4. United States Court of Appeals,for the Fourth Circuit, In Re: Under Seal, no. 13-4626, 2013.
5. United States Court of Appeals for the Third Circuit, U.S. v. Apple Macpro Computer, 2017, no. 15-3537.