Paakat
Revista de tecnología y sociedad

Recension. Technology damage law, cybersecurity and Insurtech

Recensión. Derecho de daños tecnológicos, ciberseguridad e Insurtech

http://dx.doi.org/10.32870/Pk.a10n19.497

David López Jiménez*
https://orcid.org/0000-0002-7013-9556
EAE Business School, Spain

Received: January 29, 2020
Accepted: May 27, 2020

Work reviewed: Jimeno Muñoz, Jesús. (2019). *Derecho de daños tecnológicos, ciberseguridad e Insurtech*. Madrid, España: Dykinson.

As evidenced by daily realities, we are experiencing a digital transformation process, which, in our daily life, makes the use of new technologies, both at a personal and professional level, an essential fact. In other words, almost every scenario of the social life has evolved towards what could be termed as *digital* by default. We ought to know how to use the new technologies (emerging technologies included) so that we are able to use them to our own benefit, which evolve at a fast pace and make those considered to be new earlier to be overdone and overwhelmed.

Without new technologies, we would not be able to refer to the digital age in no case. We should be aware and fully responsible for the use we make of them. At present, there have been important innovations and unimaginable advances in a short time. Do think, for example, about the *big data*, the *Smart contract*, the *blockchain*, the *bitcoin*, the platforms of collaborative economy and a very long etcetera.

The book which is the subject of this review has a very accurate systematic content and structure. It includes three chapters with full technical and legal knowledge to limit the field of the law of torts in the technological field; likewise, it analyzes the relevance of cyber security as an essential instrument to manage technological hazards and, in addition, its financial transference in view of the innovations included by *Insurtech*. The latter and innovative word refers to the sector including traditional insurance companies, those of technological nature, and to recent disruptive *startup* companies which, by definition, resort to new technologies.

* PhD University of Sevilla, and PhD Rey Juan Carlos University, Spain. Full Professor at EAE Business School, Spain.

Among new technologies, they must be considered among many others, the chain of blocks, cloud computing and the like. With this, new forms of supplying products and services to the end customer are created in the insurance sector. It would seem, *a priori*, that *Insurtech* is, to put it in colloquial terms, a sort of poor brother of *Fintech*, which refers to financial technology, and which has attained noteworthy attention globally. The so-called *Fintech*, as is known, has technological instruments that enable the realization of diverse legal acts linked with money, in a broad sense.

Chapter one of the book refers to cyber-risks and their impact on worldwide social-economic development. In the first term, technological and cybernetic risks are analyzed, and make a stop at the concept of and evolution of cyber-risks aimed to center on the history and operation of the network. The increase and progress of cyberspace have made it possible that the threats of comprising systems could have an impact on a large number of situations, actions and subjects. Thus, they would be dubbed as threats to national security when they imply a risk to public order, the population or the systems and structures of strategic nature which are essential for the operation of the society, as is the case of critical infrastructures.

Failures and weaknesses of critical infrastructures comprise the most significant example of cyber-threat, which may become manifest in view of hyperconnectivity. In addition, these damages may remove limits and barriers and, so, disseminate throughout the system. For this reason, security of each individual system, which is an inherent part of the digital ecosystem, aids in creating a strong cyberspace, which favors common interest of every subject who is a party thereof.

The author studies goods and legal rights that may be affected by situations and activities occurring in the cyberspace, so that they would later adjust and conceptualize the law of torts in the cybernetic area. Also, the legal aspects of securing the different realities of cyberspace and the effects of insurances as a tool within the reach of the civil society to maintain justice are examined. In the second place, the repercussions of the hyperconnected world are studied and, specifically, cyberspace and digital ecosystems.

Chapter two refers to the field of cyber-risks. In the first term, it analyzes the appearance of damage in cyberspace and its protection. It must be mentioned that by the end of 2013, the representative of the European Union for Foreign Affairs and Security Policy said that the same standards, principles and values employed out of the virtual world should be enforced (which may be extended to the European Union) so that cyberspace will continue to be open and free. It is therefore necessary to safeguard fundamental rights, democracy and the supremacy of law in Internet. In this respect, the European Union is cooperating with its international partners, the civil society and the private sector to foster these rights from a global perspective.

Moreover, several issues linked to national security are analyzed, such as public concern in cyberspace, or cybercrime and, lastly, cyberterrorism. Under the cybercrime concept, the author refers to identity theft, online fraud, scareware, fiscal fraud, business theft, extortion, customer data theft, industrial espionage, and intellectual property theft. Reference is made to the fact that regulations related to cybersecurity that have been approved by Spain are greatly centered in the protection of personal data and in pursuing crimes, the execution of which implies the use of computer environment.

As foreseen, the work fully analyzes, cyberterrorism, which may be conceptualized as the use of IT systems to attach critical infrastructures or public administration systems, or coercion or intimidation capable of affecting the public sector and civil society.

The end goal of cyberterrorists is to spread terror, by creating disturbances, chaos and every damage possible. Cyberterrorists form criminal groups who, regardless of their better or worse financial means, diligently operate to attach their objectives. They have the skills to infiltrate in a number of Internet sites and services, to enter in a number of systems for the appropriation of confidential information and, later, sell them or make them public. In addition, they steal from financial entities to face their criminal activities to the full extent; in a number of occasions, they corrode information and infrastructures to disrupt or simply to destroy.

Within infrastructure attacks, we can, among many other assumptions, refer to two cases where the electric power supply in Ukraine was affected by cyberterrorists. One of the major threats worldwide is nuclear plants. Cases occur and they are not isolated events. By the end of 2019, India recognized that their nuclear plants have been attacked by cybercriminals from North Korea. In this case, it was pointed out that the computer virus that affected the nuclear power plant is analogous to that of the DarkSeoul campaign, which is an espionage program directed to banking entities and South Korean media, attributed to the Lazarus Group, linked with cyberterrorists from North Korea.

Without prejudice that the author makes reference to the Internet of things, emphasis should be made, concerning cybercrime. Indeed, it may be taken advantage of by hackers with admittedly spurious ends. By the excessive rush for connectivity to the Internet of things, we have more devices connected to the network day by day; among these are, with no exhaustion, the following: webcam, video surveillance cameras, smart vacuum machines, refrigerators, voice assistants, and a very long etcetera.

We must start from the fact that these instruments have been designed and manufactured, when thinking, above all, in their functionality, and not in security. The above devices may be turned into zombie devices for multiple purposes other than their original function. An allusion may be made to the Mirai attack (October 2016), where a

network of over a million devices implemented a denial of service attack which completely affected, among others, Twitter, Github, Amazon and Spotify. The weak point of a number of devices and accessories was taken advantage of which were connected to the network. Mirai acted under a free software license, therefore it was completely simple for any person to make us thereof with the purpose of staging a denial of service attack, which affected printers, routers, or webcams. A very large number of devices and accessories work on a predetermined user and password. Malware takes advantage of this, it infects them and takes control thereof.

U.S. entities recommend users of devices (such as those mentioned above) that it is mostly convenient that they isolate those devices in a secondary Wi-Fi network, that is, different from the one they use to link their vital devices, such as portable devices, computers, and smartphones. Therefore, if attacked, this would prevent that, from this device, they may access other main devices of users.

Moving on, the author studies data incidence in this subject matter and, specifically, the protection of non-material goods, and the legislative aspect of the protection of data of personal nature. In this chapter, critical infrastructures, Internet of things and insurance problems, in view of autonomous vehicles, are also the object of examination. Under the latter item, it is likely that future insurance of autonomous driving takes producers and maintaining officials of motor vehicles to concur or partake in subscribing transit insurances which, in the light of recommendations by the European Parliament, it seems that they will continue to be compulsory.

Some specialists foresee that invoicing in this sector shall have a striking fall; in addition, they say that it shall be manufacturers who will stipulate the policies and that they will include, among other clauses, the dangers of having a hacker attack. Legal responsibility, in the event of an accident, shall not lie on the driver, but on the manufacturer of the vehicle essentially; in other terms, it shall be manufactures who have to insure the vehicle. On the other hand, with regard to what is presented therein, the search for energetic efficiency shall cause, especially in the largest cities, the implementation of companies engaged in comparative mobility services, such as car hiring companies for short periods of time.

It is likely that, with ongoing changes in the subject matter at hand, getting insurance premiums will be reduced in the European scenario. The latter contracts would amount between 10% and 30% until the year 2025, which could result in an invoicing reduction down to 35 billion euros for these companies. A business collapse, which will undoubtedly result in mergers, and even in the shutting down underwriters who are not so capable to adapt change to the new prevailing times and models.

One of the several advantages of autonomous vehicles lies in the fact that technology allows that the human factor be suppressed, who is considered to be

responsible for approximately 90% of accidents. Although it is likely that technology may give rise to an increase in the amounts of indemnities (both of vehicles and their repairs, in their different variations, will rise), the total amount will be reduced as a consequence of the minimal number of accidents. This, from another perspective, is negative news to traditional insurers which, by the way, cannot disregard another innovation which, in view of technological change, experts predict the arrival of new agents in this sector.

Finally, the chapter closes with two highly significant questions, emerging damage and loss of profit, as well as the loss of reputation, and harm of honor of natural and legal persons, and which result from a cyberevent of any type.

Individual or collective cyberattacks pose a relevant risk to companies and institutions, not only from the economic point of view but also regarding reputation effects. At present, a number of organizations do not have communication protocols in place to face these cyberattacks. It is paramount to have a cybernetic insurance which, in the event of an accident, faces payment of costs for engaging image and brand consultancy services to mitigate the crisis which may have eventually been caused.

The last chapter deals with cyber-insurances and the effects of cyber-risks of civil liability insurances. Assistance instruments to drive, as well as driving autonomous vehicles limit human risks linked with driving, but at the same time give rise to a new generation of risks. At present, the automobile industry is holding discussions about the scope of liability from driving motor vehicle, for the meaning of autonomous driving is not unanimous. This dispute consists in explaining whether the autonomous driving system is driving assistance (which needs the active participation of the driver) or whether, on the contrary, it completely replaces the driver.

There are elements such as autonomous or assisted vehicle driving, which reduce human risks associated to driving, although simultaneously, they fit in a new generation of risks, where it seems to alter the application of the events of civil liability in accordance with the traditional events. As further determined by the author, in the field of cyber-risks, there is a series of elements which, certainly, shall give rise to discussions on the application of an unforeseen event and force majeur.

The insurance industry ought to adapt to the circumstances brought by information technologies in social, economic and entrepreneurial matters. Thus, the network creates a means, in view of which, new relations are created and new services supplied. Also, getting advantages is admitted for traditional activities and relations. We are referreing to the fact that more businesses are gradually including technological systems with the purpose of optimizing their results, and, at the same time, create new products and services with an important technological component.

This industry has managed to lower the cost of their products and services in view of technology, which has improved the processes implied thereby. Moreover, technological advances have allowed them to be keep up and guarantee the wellbeing required by a customer. The most usual damage, and which poses the most harm to a company, is the damage to computer equipment and data processing. Within the classification of unwanted actions that may occur, there are viruses, data theft, extortion and fraud, which comprise the most relevant cyber-risks faced by companies. The medium value of these actions to companies affected thereby, in the specific case of Spain, is about 50,000 euros. Now then, this is not the main handicap, as the worst that could imply for a place to close is that it is not well protected (both from the technological and economic perspective).

Technological defense, in principle, goes through what is called, in popular terms, cyber-hygiene. With this term, it is sought to safeguard healthy or preventive habits in topics of cybersecurity, such as strong passwords, avoiding downloads and unsafe websites, among a number of other actions. It is paramount to have proper technical measures: antivirus, firewalls and permanent updates should be considered.

Yet, whatever the efforts and the investment, we have to bear in mind that there is no zero-risk. It is significant to also have economic protection; although the wrong effects of the attack cannot be completely avoided, the impression can be minimized. Cyber-risk insurance is the last resort in the defense of attacks, infringements, and theft of information of the company. They provide a high degree of legal and economic security, in respect to resulting liability. Based on the scale of the incident, a cyberattack shall imply expenses resulting from managing the crisis, in the first term, civil liability, legal protection, loss of earnings, reputation harm, and eventual payment of fines.

Regarding sanctions, one of the elements with greater repercussion is the duties of every company in respect to processing personal data of its customers, which results from the amendments to the European Data Protection Regulation, which is a direct norm that does not require transposition to countries of the community.

A section of the insurance where the provisions have had strong premium increases is cyber-policies, with which the organizations are seeking protection from technological attacks. Penetration of new technologies has affected the insurance industry in two areas: in the first term, whilst companies where digitalization has rampaged the processes and where large bags of critical data accrue, and as defense providers, which gives rise to a new and promising activity area. For this reason, cybersecurity is mostly relevant in this sector than in any other sector.

At present, there are over a hundred insurance companies worldwide which supply services to face cybernetic risks, in addition to the fact that they absorb the dangers to customers when an attack is produced. To security system integrators, there

is also the possibility to optimize cybernetic security as this insurance is presented as proof so that its customers become aware of their unrelenting security protocols. The existence of cybersecurity threats shall increase with the growth of the Internet of things.

For these reasons, companies, security system professionals included, ought to inquire about the benefits of cybernetic liability insurances. As is known, the greatest benefit of these products is to enjoy peace in the assumption that corporate data or information has been violated, which is a traumatic experience.

From political revolts and the fast changes of technology, a number of analysts believe that a large-scale cyberattack could occur at any time. Cybersecurity is at the front end of the concerns of economic operators and of the public sector; however, coverages shall only be effective if there are collective solutions to properly face the risk. As the cybernetic insurance markets mature, we ought to find out whether these policies shall be compulsory –such as those in Spain for civil liability, adapted to the different scenarios–; this would facilitate the supplementary degree of security to companies and customers.