Some Reflections on Cybercrime. Managerial and Law Implications in Italy

Author Details: Antonia Rosa Gurrieri
Department of Law, University of Foggia
Largo Papa Giovanni Paolo II - 71100 Foggia- Italy
Email: antoniarosa.gurrieri@unifg.it

Abstract
The growing interest on cybercrime is related to the rapid diffusion of digital technologies. The necessity of a due diligence protocol for all countries is one of the main goals of European Commission and all states in the world. This behavior could avoid cross-border damage.
The aim of this work is to give an overview on the main fields of investigation that are directly affected by cybercrime.
Keywords: *cybercrime; legal aspects; digitalization process*

1. Introduction

Technological and digital innovation presupposes an acceleration of the entire info-environment and a radical change in governance models. While it is true that innovation is proceeding at an exponential rate, it is equally true that placing it in an appropriate regulatory context is the essential step to ensure its proper functioning. In other words, it is a matter of reconciling ethics and governance so that the importance of a moral evaluation could be read through the connection between digital governance and regulation. While digital governance concerns the proper use of information, digital regulation introduces ethics and moral signs to define good practices. The aim of digital ethics and governance includes cyber and cyberattacks (e.g., effects of the attacks suffered by DNS provider Dyn in 2016) as they involve government, private sector, providers, international relations, etc.
Paragraph 2 discusses the literature that deals with this topic, while paragraph 3 underlines the main entrepreneurial limits connected to smart crime. Paragraph 4 tries to frame the legal aspects and paragraph 5 presents a brief conclusion.

2. Theoretical background

Hughes and Colarik (2016, p. 2) argue that "firstly, cyberwar involves actions that achieve political or military effects. Second, it involves the use of cyberspace to deliver direct or cascading kinetic effects that have outcomes comparable to traditional military capabilities. Third, it creates results that cause or are a critical component of a serious threat to a nation's security or are conducted in response to that threat". The direct consequence is that a cyber operation can be considered a criminal act (act of war, or cybercrime).
In the context of ethics and morality, it is necessary to include information and digital technologies since Industry 4.0 (I4.0) and the digitalization process bring the globalized world in a "smart moment" that is able to instantly change the method of connection. In this scenario, also the value chain and production require a process of smart adaptation.
In recent years, the process of globalization and digital transformation of industrial production has also changed economic systems, generating a considerable impact on the functioning of markets and people's lives, in a changed socio-political context. The sharp increase in market extension has followed the pervasive globalization process and the recent smart opportunities dictate a new path of production that share in real time a multitude of data by networking multiple organizations through web-based connection of machinery, products, workers and consumers. This is the concept of I4.0.
Innovation, as a result of the integration of science and technology, is increasingly transversal and has a widespread simultaneous effect on products, processes and methods and radically changes the relationship between producers and consumers (Morelli *et al.*, 2020). Digital technologies (Internet, robots, automation, machine-to-machine intelligent production) take a potential technological unemployment, due to an unskilled workforce and robot substitution.
One of the advantages of automation is the rapid reorganization of cheaper and smaller production runs. Intelligent, customized products include a deep understanding of the entire production process and consumer

applications and make their way independently through the supply chain. The aim of the automation pyramid towards self-control systems is to extract, visualize and utilize large amounts of data.

The development of algorithms for data management is one of the main challenges of the digitalization process, as the pervasive integration of components easily generates big data systems. By facilitating information and knowledge, IoT improves the efficiency and effectiveness of knowledge development and management. However, the disadvantages of heterogeneous data can undermine industrial development, but Big Data management can help mitigate the problem (Morelli et al., 2017).

The use of artificial intelligence and technologies also entails a new vision of organizational culture. Creativity and result orientation increase, and managerial innovation implies rapid approaches to time-to-market through the creation of intelligent, flexible and qualified production structures, able to gradually facing heterogeneous markets. Therefore, all industrial workforce (employees and managers) must be technologically qualified.

3. Managerial aspects

In a global market with a rapid circulation of knowledge flows, high risk capital and labor factor mobility, the dominant service logic becomes disruptive due to the increasing use of data-intensive technologies in open innovation systems.

The interaction of the virtual and real worlds determines the fragmentation of production into multiple global value chains. The result is a digital, flexible and adaptable environment. Inside the black box, in a cyber-physical atmosphere, business operators interact with each other through a complex network of machines, physical assets and digitized devices (Morelli et al., 2020). Entrepreneurs have to manage their existing organization in real time and the digitization of markets and the tools of I4.0 represent an opportunity to adapt the organizational system of the enterprise. Artificial intelligence modifies the current process control system (Porter and Heppelmann, 2014) by overcoming the traditional approach to production planning and control and achieving different levels of performance, where setting up simple monitoring tools would help achieve the most complex objectives.

Industries have experienced profound structural changes in the organization of production. In particular, manufacturing industries have moved from mass production to customized production, recognizing a strategic competitive advantage in the ability to provide products and services individually designed for each consumer. In relation to small and medium-sized enterprises, a step-by-step approach could be useful for the improvement of instrumental skills: analysis of the decision-making process (monitoring); use of algorithms for the analysis of historical data (control); analysis of monitoring data and consequent autonomy of behavior (optimization and autonomy).

Furthermore, since synchronization of flows along the entire supply chain (flexibility) is one of the main objectives of digital integration, CC platforms could be used as collaboration structures between firms. At the level of production plan algorithms by predicting internal flow disturbances and variations in consumer demands, it would be possible to hypothesize an increase in productivity, as the estimation and use of algorithms reduces planning time, promotes collaboration between all network partners and facilitates the synchronization of all production processes. Simulation models for SMEs have been proposed in the literature: i) Denkena et al. (2014), start from the idea that most SMEs do not have reliable data to introduce IoT and RFID technology to manage flows and facilitate the implementation of Lean Manufacturing. ii) Constantinescu et al. (2015) develop Just In Time Information Retrieval (JITIR) to eliminate the problem of excess data flowing into the IoT. iii) Barenji et al. (2017), on the contrary, present the Prometheus method to develop a software application for the simulation of planning, based on dynamic demand and production variations; iv) Givehchi et al. (2015) report that SMEs apply cyber physical systems for production planning and control, registering, however, a limitation in the low level of in-house skills, and especially in the low capacity to process complex algorithms.

A strong co-ordination capability permits to spatially separate production phases and to integrate data.

With regard to organization, the main problem is that intelligent systems based on decentralized and automated self- clash with the traditional pattern of production, resulting the paradox of (organizational) inertia. The limited resources of SMEs could be surpassed by a networking system.

Moreover, a collaborative environment could be implemented to increase SMEs' flexibility. In fact, it permits to share each simple resource while reducing risks. Consequently, all involved firms can face the

volatile smart markets, and also the availability of different product in a network could optimize the complete production process. However, while information sharing may lead to innovation, it may also generate asymmetric effects due to opportunistic behavior and higher coordination costs resulting from antagonism and competition between firms.

Maintaining global competitive advantage occurs in collaborative networks, for the individual unit through the maintenance of core competencies, for the group through the outsourcing of other activities. While in traditional models the key characteristics of networks are generative knowledge and cognitive clusters, in the digital era, operational supply chains that manage the multi-localized and interconnected transformation of intangible products and services could be the key element.

When a company uses I4.0 tools to operate new management strategies, it assumes that it is open to cultural change. The acquired knowledge, which represents the social capital of the enterprise, using Big Data and IoT can be global. As a result, smart companies have to cope with a persistent increase in the knowledge content of outputs, reinforcing the importance of intangible assets in production. Moreover, skills gaps in human capital formation remain one of Italy's main problems, both for workers and managers. This lack would accelerate trends towards automation in some cases but would also block the adoption of new technologies and thus hinder business growth.

In the near future, if industrial policies are not supported by ad hoc supply-side interventions, the gap between employment and productivity will increase, amplifying social inequalities. The creativity and flexibility of human beings will be an added value.

4. Legal Aspects

Computer crime is not a category that has a specific definition; at the same time, there is no unambiguous definition of computer crime or cybercrime in international law.

As a matter of fact, cybercrime encompasses various forms of conduct that harm interests that are protected under criminal law: they fall under computer crime, which many national legal systems regulate.

With the development of the Internet, the computer is increasingly conceived in a collective dimension, as the potential for global interconnection has meant that the individual perspective of the networks used has been overcome.

Basically, organized crime under the cyber profile includes, on the one hand, computer crimes in the strict sense (i.e., cases involving the automation of data and information or of technological relevance); on the other hand, computer crimes in the broader sense (i.e., specific cases that only apply to acts committed with the use of technology, the network or cyberspace).

The Council of Europe's 2001 Convention on Cybercrime has precisely the purpose of promoting a common policy, from a criminal law perspective, with the aim of protecting society against cybercrime phenomena, through specific legislation using cooperation logic at international level.

In this work, reference is made to different types of cybercrimes, including both those in the narrow sense, which include situations in which the technological aspect appears central and has implications concerning networking or the use of cyberspace; and cybercrimes in the broad sense, in which the concrete possibility of networking is present. The latter, in particular, can disregard the cyber aspect, which is why they are formulated in more general terms.

The entry into force of the Lisbon Treaty, which dates back to 1 December 2009, marked the beginning of a strong relationship between criminal law and the European Union. In particular, Article 83 of the Treaty on the Functioning of the Union (TFEU) entrusts the European Parliament and the Council with the power to establish minimum rules concerning the definition of criminal offences and sanctions in the area of serious transnational crime (Rigotti, 2022).

Cybercrime falls squarely within this ambit, referring to serious criminal phenomena with transnational relevance. If a recall is made to attacks perpetrated on companies, it must be emphasized that they bear numerous risks, which can compromise business life, with regard to IT tools and, above all, to data, people, and services.

In particular, small and medium-sized enterprises risk not only the loss of data or major frauds, but also the loss of know-how characterizing the Made in Italy brand.

In this regard, specific training of the management body can well counteract the phenomenon. In fact, managers operating within Information Technology, at present, hardly perceive a loss of data as a damage with economic significance.

It is necessary, on a global level, to promote a wider knowledge of the phenomenon, in particular among directors and shareholders, so as to determine the activation of appropriate countermeasures and policies. These include, on the one hand, the sharing of information and the creation of networks between companies, specifically in the same sector or of a comparable size; on the other hand, the sharing with trade associations, financial institutions and law enforcement agencies, to promote specific countermeasures leading to the mitigation of the damage suffered.

In general, the smaller the size of the company, the more difficult it will be to recognize attacks compared to larger companies, either because they are operating units that are unlikely to have departments specialized in such technical aspects or because the threats are more difficult to detect for such companies.

Organized crime, in particular, does not in reality discriminate against attacks with respect to the size of the targeted company. Our territory is significantly affected by cyber threats: the assumption is that this is encouraged by the consideration of the Italian language as the ninth most used language in the world for spam e-mails; if we consider, instead, the countries that have recorded the highest number of malicious apps (within the Android platforms), Italy is fourth-

The cybercrime phenomenon in Italy is not reflected in official studies and statistics: instead, data processed by the private sector are available. In particular, Clusit, an association founded in 2000 at the University of Milan (Department of Informatics), deals with the dissemination of the culture of cyber security, also ensuring the sharing of sector-specific information.

Clusit draws up an annual report on ICT security: the latest findings show that cybercrime is a rapidly and worryingly growing phenomenon.

Attacks have increased both numerically and in terms of the value of the data stolen.

Cyber criminals are more likely to attack small companies that provide goods and services: this is believed to be a means to reach medium- and large-sized companies, hitting first those with lower levels of cyber security, for cultural and budgetary reasons.

In any case, cybercrime, in reality, affects all businesses transversally and indiscriminately, and is not confined to those that are part of the IT sector or enjoy highly specialized conditions. In many cases, companies appear reticent in disclosing information about attacks they have suffered and sometimes even find it difficult to verify that the attack has taken place.

5. Conclusion

The international economic scenario has changed, shifting the basis of industrial competitiveness into a dynamic competition, where it is appropriate for governments, companies, private organizations, etc. to improve their learning capabilities and create smart knowledge. The digital process is the way to create new value.

The fields of investigation and the ways by which cyber criminals act are many and different:

- Supply chain analysis and logistics: smart technologies present an efficient supply chain thank to a rapid up-to-date information, able to mitigate the bull whip effect and to reduce the inefficiencies of the supply chain.
- Security and privacy: Internet and smart technologies in general increase the risk of information's intrusions. This danger needs to raise informatic and digital barriers to protect not only industrial bur also all other systems from cyber-attack.
- Smart infrastructure: digital technologies bring efficiency, flexibility, reliability and reduced operation costs. A smart environment includes intelligent activities, logistics and mobility.
- Healthcare: smart devices enable consumers and patients to rapidly send health-information to their doctors. These are granular and integrated systems that are considered automated because they use Big Data and IoT.
- Society: Cyber bullying.

References

Barenji, A.V., Barenji, R.V., Roudi, D., Hashemipour, M. (2017). A Dynamic Multi-Agent-Based Scheduling Approach for SMEs. The International Journal of Advanced Manufacturing Technology 89(9-12), 3123–3137.

Constantinescu, C., Mattoo, A., Ruta, M. (2015). The Global Trade Slowdown. Critical or structural?. World Bank Group. Policy Research Working Paper 7158.

Denkena, B., Schmidt, J., Krüger, M. (2014) Data Mining Approach for Knowledge-Based Process Planning. Procedia Technology 15, 406–415.

Givehchi, M., Haghighi, A., Wang, L. (2015). Generic Machining Process Sequencing through a Revised Enriched Machining Feature Concept. Journal of Manufacturing Systems 37, 564–575.

Hughes, D. and Colarik, A.M. (2016). Predicting the proliferation of cyber weapons into small states. JFQ, 83(4), 19-26.

Morelli, G., Spagnoli, F. (2017). Creative Industries and Big Data: A Business Model for Service Innovation. In: Za, S., Dragoicea, M., Cavallari, M. (eds.) Exploring Services Science, pp. 144-158. Springer, Berlin.

Morelli, G., Pozzi, C. and Gurrieri, A.R. (2020). Industry 4.0 and the Global Digitalised Production. Structural Changes manufacturing. Chapter 13. Springer Science and Business Media LLC.

Porter, M., Heppelmann, J.E. (2014). How Smart, Connected Products are Transforming Competition. Harvard Business Review 92, 64–88.

Rigotti, C. (2022). A long way to end rape in the European Union: Assessing the commission's proposal to harmonise rape law, through a feminist lens. New Journal of European Criminal Law. 2022;13(2):153-179. doi:10.1177/20322844221100046