VDA LISBON HEADQUARTES

In the era of technology, data are growing exponentially, as does the rate at which organizations share data through online networks. Billions of machines – tablets, smartphones, ATMs, security installations, environmental control systems, and many more – are all linked together, increasing inter-dependencies. And 5G is just around the corner.

by patricia cardoso

DIGITAL ALARM

The report "Prepare for the expected: Safeguarding value in the era of cyber risk", made by Aon company, forecasts that losses from cyber attacks will reach €6 trillion globally by 2021.Two lawyers that work everyday with Cybersecurity talked about the long road to legislation, how it is working and what to expect for the future. Because one thing is certain: Cybersecurity has arrived and it's not going anywhere.

Organizations are increasingly opening their IT systems to a wide range of technology and lose direct control of data security. Cybercriminals are very aware of these vulnerabilities. Driven by a wide range of motivations – from pure financial gain to raising the profile of ideology, to espionage or terrorism – individual hackers, activists, organized criminals, and governments are attacking government and company networks with increasing volume and severity. Not all organizations are necessarily easy targets for cybercriminals. For example, a small or midsized company has a very different risk profile than a multinational organization. What is true for any government or organization is that cybercrime risks can be controlled. Cybercriminals are not invincible forces, and while they can cause real damage, the Law has made some signs of progress in developing mechanisms to protect the companies and individuals.
The issue of Cybersecurity can be considered a recent one when talking about a central concern in European regulation. For a long time, the focus has been more on technological innovation than on the security of equipment, products, and services in the digital environment. This concern increased when "the single European digital package called 'Single Market' was negotiated and approved by the European Commission," recalls **Magda Cocco**, partner at Vieira de Almeida (VdA) and head of Communications, Data Protection & Technology. VdA began working on data protection in 1990. The first European directive is from 1991. Portuguese law predates the directive.
The regulation about General Data Protection final text has been in force since May 2019.
The regulation comes at a time when it was necessary to ensure "the competitiveness of Europe in technological terms, concerning other parts of the world such as the United States and China in particular. One of the pillars of this package is the security of digital networks


MAGDA COCCO

"IT IS IMPOSED IN ALL MEMBER STATES AND DEFINES SPECIAL SECURITY OBLIGATIONS IN THE NETWORKS AND INFORMATION SYSTEMS OF ENTITIES THAT ARE CONSIDERED CENTRAL TO THE FUNCTIONING OF ANY ECONOMY"
Magda Cocco

5G. The future of cyberattacks?

Magda Cocco (*pictured*) talks about the concerns raised by this technology. "5G is now going to be launched in Portugal and one of the major concerns is to ensure that the systems that make up the entire 5G chain end up exposing much more a set of services that are still in the analog world. The internet of things. All things connected. There is a huge discussion in Europe between creating two many restrict laws that can stop innovation".
Ricardo Henriques agrees but points out that there are increased functionalities in all the devices we have at our disposal and the speed of data transmission of 5G, brings new potentialities, new productive capacities, and interaction with all those equipments but on the other hand it brings increased risks on protection ones data and privacy as we expect to have all things connected, like vehicles, phones, house devices, prettty much anything.

and services. Because studies were made to know why Europe did not have the same level of success in the global digital economy and one of the factors that were pointed out was the lack of security of our digital media. It required all companies and all industries to report digital security accidents within 72 hours to data protection authorities. This is when it comes to personal data. For example, a database from a bank, a hospital," she says.
Data protection regulations apply to European companies or companies that offer services to European entities, they have the extraterritorial component. "Any company that wants to provide digital services to European citizens or monitors the Internet behavior of European citizens is also subject to this regulation," she says. In other words, an American company does not need a European presence to follow the rules. In the limit, there may be a penalty and a fine imposed on that company.
Magda also points out that "at the European level, in addition to the general data protection regulation, legislation on essential infrastructure has also been strengthened, which also provides for security measures. It is imposed in all member States and defines special security obligations in the networks and information systems of entities that are considered central to the functioning of any economy. The Cybersecurity Act, the Cybersecurity code that establishes the certification of technological equipment, has been passed. It is optional for companies. And a very important one, ENISA, the European Cybersecurity Authority has been approved, entity managing all Cybersecurity topics at European level," she says.
Ricardo Henriques, a partner at Abreu

"A HOSPITAL THAT IS CYBER-ATTACKED AND A FILE IS LOST. THE LAW REQUIRES THAT THERE BE ALTERNATIVE DATABASES TO RESTORE THIS SITUATION. THIS WAS NOT THE CASE BEFORE. NOW THERE ARE SECURITY OBLIGATIONS IMPOSED"

Magda Cocco

"IN THE PORTUGUESE CASE, THE NATIONAL CYBERSECURITY CENTER HAS FINALLY, I WOULD SAY, BEGUN TO OPERATE EFFECTIVELY, PRODUCING SOME VERY USEFUL DOCUMENTATION FOR COMPANIES TO TRAIN IN THIS AREA"

Ricardo Henriques

Advogados, guarantees that the European Union has made a great effort in the construction of Cybersecurity systems "In the Portuguese case, the national Cybersecurity center that has finally, I would say, begun to operate effectively, producing some very useful documentation for companies to train in this area, with a national Cybersecurity framework, with a roadmap of minimum capacities for Cybersecurity, documents that are available on the official website and give a map, a very concrete guideline, with very concrete measures on what companies have to do to train in this area of what they have to do."

However, it is necessary to forget about those movies about cyberattacks. Magda says that "nowadays, there is a much more advanced level of sophistication, which makes the authorities work difficult. There is an industry behind it with the most diverse purposes, like making money out of ransoms, paralyze companies, or to have access to business secrets, to name a few. In the middle, there is a concern to inform other lawyers in other areas about the reality of Cybersecurity." There is already an industry to attack and redemptions are a very common situation, in exchange for the publication of data.
"There are currently several companies that have problems related to Cybersecurity because they have not invested enough in protecting their systems or because they are starting to invest now but do not have the proper systems to protect from the speed with which cyber attackers are also able to update their attack capabilities or because, simply, the systems, even those in which they invest, are not inviolable because there is not a 100% defense capability," defends Ricardo Henriques.

Prevention. Firms need to act on it

Ricardo Henriques (*pictured*) explains what the National Security Centre advises all companies and inviduals to do. Some of the good practice recommendations are the issue of the passwords that people use and which is in fact news every year from the lists of the worst passwords used and that people keep repeating the passwords and using unsafe words is finally that simplest measure, but then many other things also related to the physical security of equipment. Also, it is important not to leave computers unlocked, not connecting to safety nets that are not safe, having at the bottom some hygiene measures to try to avoid unnecessary risks because there are already risks, even for those who take those measures, because there is no infallible or 100% safe system. "There are already risks for those who take all the precautions. The question of answering emails when they do not know where they come from, opening attachments that they do not know if they are safe, not having an anti-virus, not having the firewalls, at last, those basic things that today are easy to implement and do not have such a high cost for the ordinary citizen, for companies, there are also solutions," he says.

"THERE ARE CURRENTLY SEVERAL COMPANIES THAT HAVE PROBLEMS RELATED TO CYBERSECURITY BECAUSE THEY HAVE NOT INVESTED ENOUGH IN PROTECTING THEIR SYSTEMS"

Ricardo Henriques

VdA has around six to ten national companies per week requesting the evaluation of data protection breaches. More than half of them have to do with cyberattacks. While some years ago there were sectors that were heavily penalized by cyberattacks, such as banking, in the first place, today this is no longer the case. Any company is exposed to an attack and a ransom demand. With this growth, the firm is focusing on prevention and advising companies, which makes more legal sense. "When they buy equipment, we follow the whole process and make sure that they comply with all security precautions and requirements," says Magda.
Also in Abreu Advogados, their clients look more for a technical component, such as "Cybersecurity specialists, technicians with the capacity to assemble their systems and their defenses although we already have some clients who come to us for the most procedural part for the search of some specific regulation by sector or by area," Ricardo says. The firm also advises clients when there is an incident and it is necessary to assess what has occurred to know if any kind of notification is necessary, either in the area of data protection or also an issue that there is also the notification for the effects of the data breach issue for Cybersecurity purposes.


RICARDO HENRIQUES

The spectrum of clients of the firms ranges from finance and retail banking, healthcare, pharmaceuticals, technology companies with online services or equipment for companies or consumers. These are companies that have products that are exposed to cyberattacks because they have a technological component for online use or that provide services or products that have very sensitive data or in regulated areas.
Ricardo Henriques recalls that "hospitals today have very complete information systems and work with all this data in these systems and this represents a risk. One of the first fines of the National Data Protection Commission on the subject of the general data protection regulation was related to the lack of security measures implemented by a hospital." For Magda Cocco, the health sector is protected by general health regulation. "A hospital that is cyber-attacked and a file is lost. The law requires that there be alternative databases to restore this situation. This was not the case before. Now there are security obligations imposed. Not least because centralizing everything in one place is a huge danger. There is also an obligation to keep the data private, so in case of disclosure, if negligence is proved, there may be compensation for the individuals. People don't know that."
However, there is always the difficulty of following a viable digital footprint and catching those responsible. The partner at VdA says: "I'd say it's one of the main problems, yes. The evidence or identification, the ability to then also reach the perpetrator at the bottom, because it can be in a completely different jurisdiction, mediated by various issues that make it difficult to reach the identification of the real person and eventually you get to an intermediate step but not the perpetrator and that's a pretty complicated part of accountability."