Chapter (X)

Law 4.0 - Regulation of Robotics, Artificial Intelligence and cybersecurity

*Elena Imi, Rachel Schieber, Silvia Quintini, Fabio Marazzi**

1.1. Abstract

Artificial Intelligence, in recent years, has seen an expansion of its use in various sectors, from manufacturing to logistics, from automotive to chemical, mechanical, biomedical and Cyber Security (to which an ad hoc paragraph will be dedicated).
Automation, by reducing production costs, has also had a positive effect on the reshoring phenomenon of national value chains: indeed, by using robotic components within the production process, there would be, potentially, less and less need to delocalize production to third countries where labor is cheaper.
Therefore, the problem of how to regulate in an effective and timely manner the applications of the so-called Artificial Intelligence has recently arisen not only in Europe, but also worldwide. In February 2020, the European Commission published a White Paper on the subject, which should be followed by a legislative proposal by 2021. In the aforementioned document, two objectives are set: i) the creation of an "ecosystem of excellence" that includes research, innovation and adoption of AI solutions by the entire value chain, and
ii) the creation of an anthropocentric "ecosystem of trust", where the fundamental rights of citizens are protected, even if that imposes limits and bans to high-risk AI applications.
At the same time, the Office of Science and Technology Policy of the White House has published the “Memorandum for the Heads of Executive Departments and Agencies, Guidance for Regulation of Artificial Intelligence Applications” which aims to regulate AI applications developed and employed by the private sector.
It is therefore intended to analyze on a comparativistic level, in the context of AI, the US federal regulation, as well as regulation in Israel, in some of the industrial

applications mentioned above.
Finally, the delicate issue of the responsibility of artificial intelligence systems in the event of error or damage caused by the machine has proved crucial in recent times, to which the draft regulation devotes a specific section, addressing both the problem of the division of responsibility among the various operators and the obligation to take out suitable insurance coverage for civil responsibility, as well as the issue of the lawsuit limitation period and the amount of compensation.

1.2. European Union

The institutions of the European Union believe they have all the potential to become the world leader in secure artificial intelligence that will benefit citizens, businesses and governments through the development of a robust regulatory framework based on respect for human rights and fundamental values.
For this reason, in February 2020, the European Commission published the "White Paper on Artificial Intelligence: a European approach to excellence and trust", which should then be followed by a legislative proposal by 2021.
In the aforementioned document, two main goals are set: i) the creation of an "ecosystem of excellence" that includes research, innovation and adoption of Artifical Intelligence solutions by the entire value chain, and ii) the creation of an anthropocentric "ecosystem of trust" where the fundamental rights of citizens are protected, even at the risk of restricting or banning high-risk Artifical Intelligence applications.
Subsequently, specifically on October 20th, 2020, the European Parliament adopted three resolutions detailing how the EU must regulate Artificial Intelligence more effectively to provide a positive boost to innovation, ethical standards, and trust in technology.
Notably, the first resolution (A9-0186/2020) addresses the issue of the ethical safeguards that Artificial Intelligence, robotics and related technologies' applications will have to respect in order to ensure safety, transparency and accountability, to avoid the creation of prejudice and discrimination, to stimulate social and environmental responsibility and to ensure respect for fundamental rights.
The second resolution (A9-0176/2020) concerns intellectual property rights for the development of artificial intelligence technologies, in which the Parliament stressed the importance of implementing an effective system for further development of artificial intelligence, including licensing and new creative processes. Among the critical issues to be resolved, for example, is to determine who owns the intellectual property of something developed completely by AI.
Finally, the third resolution (A9- 0178/2020) deals with the sensitive issue of the civil liability regime for damages and injuries caused by Artifical Intelligence systems.
Contextually, the European Parliament has also set up a special ad hoc

parliamentary committee on Artificial Intelligence in a Digital Age (AIDA), whose task is to analyze the impact of AI on the economy of the European Union.
This was recently followed by a final and important resolution of the European Parliament of January 20th, 2021 on "questions of interpretation and application of international law in so far as the EU is affected in the areas of civil and military uses and of state authority outside the scope of criminal justice"[1], in which the Parliament called on the Commission to establish an EU legal framework on Artificial Intelligence, providing definitions and ethical principles, including its use in the military field.
The aforementioned text aims to ensure that Artificial Intelligence and related technologies are human-centered (i.e., intended to serve humanity and the common good).
The guidelines outlined by Parliament for the its use can be briefly summarized as follows:

1. Need for an EU strategy to prohibit weapons that are not subject to human control.
In this context, it was stressed that human dignity and human rights must be respected in all the European Union's defense activities. Therefore, it was considered that the use of Artificial Intelligence in the military and civilian fields "*must be subject to meaningful human control, so that at all times a human has the means to correct, halt or disable it in the event of unforeseen behaviour, accidental intervention, cyber-attacks or interference by third parties with AI-based technology or where third parties acquire such technology*"1.
Therefore, the use of Lethal Autonomous Weapon Systems (LAWS), which would also raise fundamental ethical and legal issues, should be prohibited.

2. Surveillance of masses and the deepfake.
The text drew attention to the threats to fundamental human rights and to state sovereignty originated by the use of Artifical Intelligence technologies in civilian and military mass surveillance.
The Parliament asked for public authorities to be prohibited from using "highly intrusive social scoring applications" (for monitoring and evaluating citizens).
In the resolution, concerns were also raised about deepfake technologies, as they would have the potential to "*destabilize countries, spread misinformation and influence elections*."
To counter this risk, according to the document, i) creators should be obliged to label such material as "*non-original*", ii) research into technologies capable of countering this phenomenon will be strongly encouraged.

[1] European Parliament resolution of 20 January 2021 on artificial intelligence: questions of interpretation and application of international law in so far as the EU is affected in the areas of civil and military uses and of state authority outside the scope of criminal justice (2020/2013(INI))

3. Artificial Intelligence in the public sector
Finally, with regard to the increase in the use of Artificial Intelligence systems in public services, particularly in health and justice, it was reiterated that they should not replace human contact or generate discrimination.
On one hand, the obligation to inform people who will be subject to an AI-based decision has been established, as well as the possibility to appeal against such decisions. Thus, for instance, in the area of justice, the use of AI technologies may help to speed up and streamline proceedings, but final decisions will always have to be rigorously vetted by a person and subject to due process.

1.3. United States

In the United States, being a federal republic, the Federation and the States maintain different areas of competence for which they have legislative powers, set by the Constitution. Therefore, the issue of Artificial Intelligence has been developed both on a federal and a local level. For what it concerns the federal response, several U.S. federal administrative agencies already have authority to regulate certain AI technologies. For example, in the U.S., civil rights laws provide for equal access to goods and services and ban unequal treatment based on race. Labor and employment laws provide for equal treatment in workplaces. Consumer protection laws protect consumers from unfair and deceptive business practices and monopolies. Privacy law help protect personal data (including biometric data). Agencies operating under the Departments of Labor, Commerce, Health and Human Services, Transportation, and Justice, can assert those laws in areas of artificial intelligence.
In addition to the above, the U.S. National Institute of Standards and Technology (NIST) is working on developing technical and non-technical standards for assessing AI technologies. This is a critical step in the future regulation of AI and reducing uncertainty by companies trying to navigate the legal landscape.
To provide another specific example, the U.S. Federal Trade Commission (FTC), the nation's consumer watchdog and law enforcement agency, enforces data privacy rules against companies that unlawfully deceive users about their collection and use of user data. Because of the value that big datasets provide, there is a temptation by some companies to collect as much user data as possible. When they do it in a way that deceives users, the FTC can sue them for violations.
The U.S. Food and Drug Administrations (FDA), currently reviews and clears AI-powered medical devices to ensure they are safe and effective. An example of FDA-cleared AI device is the IDX-DR, which uses machine learning neural network to evaluate eye retinal images for indications of retinal diseases. Critics of the FDA's

program argue that the approval process is not transparent, and the FDA does not fully scrutinize the "black box" of an AI system before clearing it to be sold.
In the area of autonomous vehicles, the National Highway Traffic Safety Administration does not specifically regulate the AI systems in vehicles but does oversee the testing of the vehicles. Other federal agencies also have programs for evaluating and overseeing AI systems (e.g., Agriculture), but no specific targeted regulations aimed at AI.
The White House issued a "Memorandum for the Heads of Executive Departments and Agencies, Guidance for Regulation of Artificial Intelligence Applications," providing guidance that federal agencies (like the FTC, FDA, others) should consult when establishing regulations or policies for how they will handle AI technologies. The document does not contain any specific proposals for how agencies will regulate, but offers general principles (fairness, accountability, etc.) and generally tries to avoid over-regulating AI (because this would impose barriers to the future development of AI). See page 8 of the document, for example.
For what it concerns federal Lawmakers' response, the Congress generally has been reactive to problems, rather than being proactive. A few recent legislative efforts may increase spending and focus on AI development at the national level. Some of these efforts may, if enacted into law, replace (preempt) state laws. For instance, the National Biometric Information Privacy Act of 2020, if enacted would replace state laws.
The National Defense Authorization Act of 2020, and the Consolidated Appropriations Act for FY 2021 both include law provisions affecting AI. These include the "AI in Government Act of 2020," and the "Intelligence Authorization Act for 2021," which will enhance government spending and research initiatives.

Moving to the States' responses, the first issue addressed by the local governments has been Privacy. Because the federal government has been slow to regulate AI technologies, the states and local governments have stepped in to regulate certain applications of AI in their respective states/jurisdictions. Facial recognition and biometric data privacy are the most prominent technology areas where states have enacted laws, regulations, or ordinances that touch on this AI technology. Currently, the states of Illinois, Washington and Texas have specific biometric data privacy laws, and several more states, including California, have broader data privacy laws. New York has proposed a biometric data privacy law similar to Illinois'. Most biometric privacy laws are self-implementing, meaning that there is no state government agency in charge of issuing regulations to implement the laws (although the laws may require a state/local government agency to handle issues involving discrimination caused by a biometric system, and the state's Attorney General—the attorney representing the state and its people—may enforce the state laws). In addition, Illinois and the proposed New York biometric data privacy laws have "private rights of action," meaning individuals who are injured by a violation of the law can directly sue the company for damages.

Facial recognition technology is another important matter considered by the local governments: it is a specific type of AI system that collects biometric data. Many states are banning or putting limits on the use of facial recognition technology. San Francisco became the first U.S. city to ban the use of facial recognition technology by police and other local government agencies. A month later, Somerville, Massachusetts, became the second major city. In 2020, the city of Portland, Oregon, became the first to ban use of facial recognition by private businesses as well as governments (law enforcement).
Another area that gets some attention is algorithmic decision systems used by state and local government agencies. No specific new regulations have been issues, and existing laws (e.g., discrimination laws) can be used to regulate.

The answer to the “How to Regulate” question remains elusive, with so many vague suggestions about legal frameworks but no concrete approaches. The European Union will probably reach a common regulation before the U.S., which should choose a national or international government-led permitting program for high-risk and medium-risk AI systems.

1.4. Israel

Israel is in the midst of a technological revolution fueled by data collection on a massive scale and by dramatic advancements in the ability to analyze and draw conclusions from data using sophisticated algorithms. The revolutionary impact of artificial intelligence and data science, research and development in industry, healthcare, security and other areas, and the anticipated expansion and accelerated progress in these areas has led Israel to escalate research and development.
As a Startup Nation, Israel has an ecosystem of excellence, innovation and a culture of technological development. The prevailing atmosphere encourages both the private and public sectors to research and use applications of artificial intelligence in manifold and diverse fields. Artificial intelligence is shaped primarily by the private sector. The Government of Israel also plays an important role in advancing applications of AI.
The Government initiative, through the "Digital Israel" body, promotes digital orientation and knowledge programs as well as “smart city” projects. Israel has various national programs using artificial intelligence, such as: the "National Digital Health Plan" and the "Fuel Choices and Smart Mobility" Initiative. In addition, draft bills have been published on several issues in this area, waiting to be discussed and enacted
Given the challenges and risks inherent in developing AI systems, and the absence of up-to-date regulations adapted to a digital world and to rapid technological changes, and cognizant of the fact that the absence of a set of ethical rules is liable

to obstruct or hamper the revolution, Israel has not rested on its laurels.

Israeli policy makers tend to view AI developments not just as a disruptive but as a transformative: AI technology is seen as critical to welfare, economy and security of Israel's citizens. Taking this as a starting point, the priority for Israel is to establish a holistic and sustainable AI ecosystem driven by the private sector with the participation of government, private industry and academia.
As of 2018, committees and workgroups have been established in the framework of the "National Initiative for AI systems,2 in which hundreds of experts across all sectors have examined technologies in the relevant economic sectors and the main issues inherent in artificial intelligence and set a goal of:

a) Building a model to ensure ethical and secure development: one that would outline the applications of artificial intelligence and foster technological innovation and scientific research and development, aligned with democratic values.
b) Building of the model would recognize that while a need for regulation exists, overregulation must be avoided that could stifle innovation, especially in the case of emerging technologies.

Accordingly, the National Initiative defined six ethical principles that will constitute the model for artificial intelligence:

1. Fairness: avoidance of bias in information, in the process and in the product.

2. Accountability: a. for the process and the decision, b. explainability at the level of the individual, the level of the collective, and the level of the developers themselves. c. Ethical and legal responsibility towards the relevant players in the value chain together with risk management, and taking of reasonable steps to avoid risk on the basis of a risk assessment.

3. Protection of human rights: bodily integrity, privacy and autonomy (ability to make informed decisions, including preventing of undue influence) and of civil and political rights (including the right to vote, freedom of expression and freedom of religion and conscience).

4. Cyber and information security.

---

[2] Nahon K., Ashkenazi A., Gilad Bachrach R., Ken-Dror Feldman D., Keren A. and Shwartz Altshuler T. (2020), Working Group on Artificial Intelligence Ethics & Regulation Report, http://ekarine.org/heb/wp-content/pubs/AIEthicsRegulationReport-hebrew.pdf

5. Safety - a) Internal safety in developing the AI tool, and b) External safety for the environment and clients while using the tool.

6. A free and competitive market.

In addition to the definition of these basic principles as the basis for characterization of AI systems, measured intervention and a self-regulation approach are proposed.[3] The idea is that self-regulation be adopted, using tools developed in the framework of the national risk assessment initiative, and advanced ethical challenges identified in the development and production stages: ethical constraints will be incorporated in smart systems, prohibited behaviors will be identified, and the ethical rules will be applied during learning and practice of the process by those working in artificial intelligence.

Instead of defining a list of activities that need to be regulated, a 3-step systematic approach is proposed:

- Mapping the various types of regulatory approaches, including their strengths and weaknesses.
- Identifying the main areas of artificial intelligence activity that could benefit from some degree of regulation, and the risks associated with each of them.
- Adapting different regulatory approaches to the different artificial intelligence activities, furnishing the Government with a roadmap to custom tailor specific regulations to each specific sector.

The following are the types of regulatory approaches identified, including their strengths and weaknesses:

a) Legislation or regulation by means of special laws.
b) Making of judicial decisions that will interpret existing legislation or fill a void.
c) Establishment of professional standards (by the Government, academia, or civil society).
d) Self-regulation by means of ethical rules or professional standards developed by the relevant professional community.

The model was proposed as a framework to help decision-makers assess the appropriate measures for the activity taking the variables into account, and not as a model to be implemented.

It was further clarified that consideration must be given to the question as to who the regulator should be, given that legislation by a central body would facilitate development of a consistent policy while risking overregulation, which could have a dampening effect. On the other hand, sectoral regulation could offer much more

[3]The committee did not deal with regulatory and ethical considerations in area of the laws of war, the assumption being that the subject will subsequently be addressed in special-purpose forums.

experimentation at the expense of uniformity in the rules.

The following 11 regulatory guidelines were proposed:

1. Adapting Israeli regulation to international legislation and standards and promoting Israeli policy in the international arena; Israel's participation in the global discussion of artificial intelligence and working towards international standards and helping to shape them.
2. Mapping the players in the field to create a fitting framework of responsibility and a system of incentives.
3. Adapting the principle of accountability to the dynamic world of artificial intelligence - examining the risks and adapting the risk management framework, observing how it works and explaining it in a precise manner, and having in place a "sandbox" before implementation in the real world.
4. Fostering normative clarity in the critical stages of the value chain of artificial intelligence products. In the preliminary stages of AI development (understanding the business need, collecting and organizing the data, building and assessing the model, distribution and monitoring), promoting regulation may mitigate risks by helping developers incorporate the ethical values.
5. A need for regular review of the regulatory policy by the regulator: a review with attention to innovation and the degree of risk associated with the implementation and uncertainties about the impact on the ethical elements.
6. Regulatory sandboxes: the idea of controlled testing is particularly useful in an AI context "because of the need to allow innovation on one hand and address unpredictable risks to social interests, on the other".
7. The interface between the proposed regulatory guidelines and the existing regulatory infrastructure 4 necessitates examination – in the light of the considerations, the interests, and the benefits to society – as to whether new regulation is required; what its scope and the emphasis should be, given what already exists in Israel, and vis a vis integration with the systems in place in other countries.
8. The Privacy Protection Authority has a sweeping and fundamental role in regulating the use of personal information in an AI context and it is therefore recommended that the Authority spearhead regulation in coordination with the other purpose-specific authorities, to examine the principles and formulate an implementation plan with respect to anonymization of personal data, a fundamental issue in AI development.
9. The Competition Authority - it is recommended that this Authority develops

[4] There are areas that have already been regulated, and in some cases are in the process of legislation or draft bills, such as healthcare, transportation, finance and education.

coping strategies to preserve fair competition in AI, protect consumers and guarantee accessibility to technology, and avoid risk and expenses for weak players.

10. The need for inter-ministerial coordination: this mechanism will ensure a coherent, consistent, and clearly defined policy that runs through all the Government Ministries.
11. Authorities responsible for information resources: it was recommended that authorities with responsibilities in information resources (used in activities affected by the products of the information processing) be required to adapt a framework that will bolster the protection of the interests regulated.

In view of the recommendation to encourage self-regulation, and the vital need for those involved in AI to take special care with regard to the inherent dangers, a two-part tool was proposed to help AI experts identify ethical risks in decision making:

a) A set of preliminary questions intended for product developers, asked throughout the chain of development and production.
b) A dynamic frequency map that helps identify the challenges in integrating the ethical values in the development stages and indicates the points at which failings have already been discovered in the past, and their prevalence.

Alongside all the principles mentioned above, it is recommended that excellence programs be built to impart knowledge and provide training in ethics, something already partially implemented in academia.

In sum, Israel is involved in international forums on ethics in artificial intelligence and human rights, and its representatives are active in European workgroups in drafting recommendations and guiding principles.5

Although a Government Decision has not yet been taken due to the political situation in Israel and the Covid-19 pandemic, a great deal of work has been done to draft a strategic and basic position that provides a response to the challenges posed by AI, and presumably, decisions in the spirit of the principles mentioned above will be taken in the near future. Some of the elements, such as building of an ecosystem of

[5]Thus, for example: Israeli representatives were active in the drafting of the OECD's AI Recommendations and guiding principles. Israel is a member of the Digital Nations (DN) and took part in a declaration on data governance:

Data 360 Declaration, https://fdfd812d-4234-49d8-8755-ff5ad565157.filesusr.com/ugd/189d02 abce8f2b8cc140e4baeec7dcab7bee97.pdf November2019.

Israel Innovation Authority, Establishment of the Israeli Center for the Fourth Industrial Revolution-World Economic Forum. Retrieved from https://innovationisrael.org.il/en/contentpage/establishment-israeli-center-fourth-industrial-revolution-world-economic-forum

excellence, are already underway, with the encouragement of the Council for Higher Education.

1.5. Cybersecurity

In December 2020, the European Commission and the EEAS (European External Action Service) unveiled a new European Union cyber security strategy. The goal is to strengthen Europe's ability to adapt in the face of growing cyber threats, ensuring that all citizens and businesses can benefit from secure digital services and tools.
Recently, namely on March 22nd, 2021, the Council adopted provisions on the cybersecurity strategy, stating that it is essential to "build a resilient, green and digital Europe."
The areas of focus identified by the Council include:

- *"The plans to create a network of security operation centers across the EU to monitor and anticipate signals of attacks on networks;*
- *The definition of a joint cyber unit which would provide clear focus to the EU's cybersecurity crisis management framework;*
- *Its strong commitment to applying and swiftly completing the implementation of the EU 5G toolbox measures and to continuing efforts made to guarantee the security of 5G networks and the development of future network generations;*
- *The need for a joint effort to accelerate the uptake of key internet security standards, as they are instrumental to increase the overall level of security and openness of the global internet while increasing the competitiveness of the EU industry;*
- *The need to support the development of strong encryption as a means of protecting fundamental rights and digital security, while at the same time ensuring the ability of law enforcement and judicial authorities to exercise their powers both online and offline;*
- *Increasing the effectiveness and the efficiency of the cyber diplomacy toolbox giving special attention to preventing and countering cyberattacks with systemic effects that might affect supply chains, critical infrastructure and essential services, democratic institutions and processes and undermine economic security;*
- *The proposal on the possible establishment of a cyber intelligence working group to strengthen EU INTCEN's dedicated capacity in this domain;*
- *The importance of strengthening cooperation with international organizations and partner countries in order to advance the shared understanding of the cyber threat landscape;*
- *The proposal to develop an EU external cyber capacity building agenda to*

increase cyber resilience and capacities worldwide".[6]

At a legislative level, however, the first EU legislation on cybersecurity is Directive 2016/1148, known as NIS 1 (Network and Information Security), which came into force in 2016 and had the merit of helping to raise and standardize the common level of networks security and information systems in the European Union.
This was followed by the EU Cybersecurity Regulation, effective from 2019, which provided Europe with a framework for cybersecurity certification of products, services and processes and strengthened the mandate for the EU Cybersecurity Agency (ENISA).
Finally, more recently, and precisely in February 2020, the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy presented a new strategy for cybersecurity. As part of this strategy, two proposals for directives were presented: the first one concerned measures for a high common level of cybersecurity across the Union (NIS 2), and the second one was about Critical Entity Resilience.
The Critical Subject Resilience Directive provides for an expansion of the scope of the 2008 European Critical Infrastructure Directive, which currently only covers the energy and transportation sectors, to all of the following sectors: energy, transportation, banking, financial market infrastructure, healthcare, drinking water, wastewater, digital infrastructure, public administration and space.

The primary objective of the proposed NIS 2 Directive, on the other hand, is to strengthen the regulatory framework for cyber security in Europe through various measures, including:

- The extension of the scope of NIS 1 by overcoming the distinction between operators of essential services and providers of digital services, in favor of a categorization divided between essential and important entities, as well as limiting the discretion of Member States in identifying those actors subject to the obligations of the Directive. Both categories will have the same risk management and breach reporting obligations. However, the supervisory and sanctioning regime will be different: essential operators will be subject to an *ex-ante* supervisory regime, while important entities will have *ex-post* supervision;
- Ensure the security of the so-called supply chains (thus aligning with the provisions of the GDPR);
- Strengthen collaboration between member states and encourage the sharing of information between the various parties involved. The Commission intends to promote the sharing of information and cooperation

[6] https://www.consilium.europa.eu/it/press/press-releases/2021/03/22/cybersecurity-council-adopts-conclusions-on-the-eu-s-cybersecurity-strategy/

between Member States, reinforcing the role of the Cooperation Group as well as through the establishment of the European network of Cyber Crisis Liaison Organizations (EU- CyCLONe), which will be entrusted with the role of coordinating the management of large-scale incidents and ensuring the regular exchange of information between Member States and European institutions. The aim is to reinforce the requirements relating to security obligations for those covered by the regulations, as well as to introduce specific provisions on the procedure, content, and timing for reporting incidents;

- Tightening up sanctions. There will be a significant increase in the penalties to be imposed for breaches of risk management measures and reporting requirements. Penalties may amount to up to 10 million euros or 2% of the total global annual turnover of the operator concerned. Current legislation, on the other hand, leaves wide discretion to member states as to the determination of the sanctions to be imposed in the event of non-compliance with the regulations and only requires them to be "effective, proportionate and dissuasive".

Finally, it should be noted that also in December 2020, the European Council and the European Parliament reached an agreement on the proposal to establish the European Cybersecurity Industrial, Technology and Research Competence Centre. The Center will be based in Bucharest, Romania, and its operations will be funded by the Horizon Europe and Digital Europe programs.
The objective of this entity will be to contribute to safeguarding the digital single market in various areas such as e-commerce and smart mobility, as well as to increase the autonomy of the EU in the field of cybersecurity. In particular, the new Centre will aim to further improve cyber resilience, to develop the latest technologies in the field of cyber security, to support cyber start-ups and SMEs, to strengthen cyber research and innovation, as well as to contribute to closing the cyber security skills gap.

Instead, with regard to the United States, it should be noted that on December 4th, 2020, former President Trump signed the Internet of Things Cybersecurity Improvement Act of 2020 that, by providing for the issuance of guidelines and controls related to IoT objects used by government agencies, represents the first step towards a broader regulation at federal level in the field of security in the Internet of Things' applications. To date, indeed, only two States have an ad hoc legislation on this issue, namely: California with law SB-327 "*Information privacy: connected devices*" and Oregon with "*Oregon's IoT Law*", both enacted in early 2020.