DIGITAL COMPLIANCE AND CRIME-PREVENTION: HOW AI AND METAVERSE MAY IMPROVE THE EFFECTIVENESS OF COMPLIANCE PROGRAMS*

Fabio Coppola**

The last thirty years could be referred to as the era of compliance. Since the U.S. Federal Sentencing Guidelines for Organization in 1991, the Italian Decree 231 in 2001 and the UK Bribery Act in 2010, different jurisdictions faced a great development in involving organizations in the prevention of corporate crimes.
This means that corporations participate through self-regulations to the prevention of corporate crimes.
There are three ways in which companies can contribute:

- **Enforced self-regulation**, which means the introduction of compelling rules for corporations with sanctions in case of violations;
- **Encouraged self-regulation**, which means the provisions of rewards as the waiver of sanction in case a corporate offence has been committed, for those companies that have adopted adequate compliance programs;
- **Voluntary self-regulation**, made of soft-law provisions, that companies could adopt or not.

Mainly Italy, but also Spain and England chose - with some differences - the second option, preferring an encouraged self-regulation[1].
It Italy, this meant the legislative provision of a catalog of crimes that could be referred to corporations. Hence, corporations would know which crimes they should prevent.
Quite interesting, the system did not oblige corporations to adopt preventive measures (or compliance programs). It was - and still is - the choice of corporations to set preventive rules against corporate crimes. Then, if a corporate crime is committed by someone representing or working in the organization, whether corporation adopted or not an adequate compliance programs makes a great difference.

* Testo della Relazione al "*6th International Forum on Persons Sought for Corruption and Asset Recovery*", Law School and College for Criminal Law Science of Beijing Normal University, Pechino (Cina), 10-11 dicembre 2022.
** Ricercatore di Diritto Penale, Dipartimento di Scienze Giuridiche presso l'Università degli Studi di Salerno.
1 See V. MONGILLO, *Presente e futuro della compliance penale*, in *Sistema Penale*, 11 gennaio 2022, p. 7.

In fact, if the corporation did no adopted a compliance programs, the crime could be referred to its negligence and a sanction could be imposed. Instead, suppose the corporation adopted ad adequate compliance programs. In that case, it could not be sanctioned as it did anything it could to prevent the crime, which should have been committed by someone who circumvented the compliance program.

In brief: if a company adopts an adequate compliance program, the crime could not be related to corporate negligence or complicity. Therefore, the corporation would not be punished.

To the purpose of this speech, it is also interesting to analyze how corporations set compliance programs.

In the first place the corporation analyzes itself, assessing the specific risk of corporate crimes in its environment and activities. For example: if a company works mainly with public officers, then there is a significant risk of committing corruption-related crimes. Instead, if the company works in the betting sector, it will mainly face the risk of money laundering.

In any case, precisely assessing the particular risk is crucial to establishing an adequate compliance program.

Once the corporation individuated which crimes could be committed and in which way, it will set rules to prevent the commission of those crimes. In other words, the organization will disclose how the company's employees and representatives will act in the risk-area to avoid crimes. In the beforementioned examples, the compliance programs would discipline how to act with a public officer to avoid corruption crimes. Moreover, it would set rules for payments and transactions to prevent money laundering.

Indeed, making clear protocols and rules that reflect the organization's best practices also greatly affects the efficiency of the company's procedures and employee awareness.

As the company made these efforts, if an employee or a representative has committed a corporate crime and it advantages the corporation (for example: in the case of tax evasion), the person who committed the crime would be punished. Instead, the company would be acquitted as it demonstrates an adequate effort in preventing that crime through a compliance program.

It is the adequacy of compliance programs that determines whether the corporation will be acquitted.

Therefore, corporations should not draw 'cosmetic' compliance programs as the copy-and-paste approach ends with the organization's liability.

However, it also means that the prosecutor or the judge will decide whether the compliance program is adequate. Reasonably, this leads to uncertainty, as it is quite hard to demonstrate that the compliance program was adequate, and that the offender circumvented it, even though the crime had been committed. Instead, the prosecutor or the judge could be attracted by the simple idea that if the crime has been committed, then the preventive program was inadequate. This uncertainty made it highly unattractive for companies to invest in compliance as they cannot guarantee their effort will be rewarded.

In this scenario, we claim the development of AI and digital compliance could be promising to the effectiveness and predictability of compliance programs in at least two ways:

a) Enforcing the crime risk assessment:

AI could firstly help companies to build compliance programs[2]. The use of algorithms guarantees a more accurate collection and analysis of corporate data. In this way, AI could enforce the risk assessment process by giving a better and customized picture of the crimes-risk in that specific company.

Moreover, digitalizing internal procedures and protocols could improve their monitoring; it also automatize the disclosure of misbehaviors and the activation of preventive rules. For example, digitalizing financial transactions could automatically impede a payment against internal procedures and protocols[3].

b) Predicting the effectiveness of compliance programs:

One of the most controversial and potential benefits of AI applied to compliance is the possibility of predicting corporate crimes and testing preventive measures.

On one way, it could sound like the 2002 Hollywood movie "Minority Report", where AI predicts individual behaviors, reports a crime before it is committed, and allows the pre-cop team to prevent its commission[4].

[2] See G. MORGANTE – G. FIORINELLI, *Promesse e rischi della compliance penale digitalizzata*, in *Archivio Penale*, 2/2022, p. 9.
[3] See G. MORGANTE – G. FIORINELLI, *Promesse e rischi della compliance penale digitalizzata*, in *Archivio Penale*, 2/2022, p. 11.
[4] See C. BURCHARD, *the "Criminal Law" of predictive society… or how "smart" algorithms (could) change the administration of criminal justice*, in *Law and Order*, 1/2020.

On the other side, the criminal compliance area could represent a promising test for predictive society. As said, the whole compliance system relies on the predictability of the adequacy of compliance programs that can assure the acquittal of companies for corporate crimes.

We also said that the main flow in the system is the uncertainty of the adequacy criteria as it depends on a case-by-case evaluation from prosecutors or judges. Only this consideration should persuade about the need for more predictability. There is also another reason for trying.

Overall, using predictive mechanisms in criminal law is risky if it allows deciding whether a specific person will commit a crime based on the input evaluated by the machine, which could contain human bias. Instead, we would use the potential of machine learning to predict whether the compliance program is effective. In this way, the predictive algorithm could bring more benefits than disadvantages:

i) **in case the result is negative** (the compliance program does not prevent the risk of corporate crimes) and the test is run before the crime has been committed, the compliance program could be integrated, and the corporation suffers no consequences (the encouraged self-regulation provides only rewards for effective compliance programs);

ii) **if the result is positive** (the compliance program prevents corporate crimes), the predictive test will help prosecutors or judges to evaluate the compliance program as adequate. This happens even though a corporate crime has been committed because the preventive efficiency of compliance program has been successfully tested through AI. Consequently, the corporation would not be sanctioned.

The AI could predict compliance programs' effectiveness using the Metaverse potential, intended as a digital twin of the real world.

The idea is quite simple. As compliance programs work in risk assessment and preventive measures, we should first create a digital database of any situational context for the crimes that the corporation could commit. In doing that, we could use statistical data and experts' opinions. On the other hand, we would digitalize the best practices to prevent the commission of corporate crimes set by corporations on the base of their own risk.

The second step is recreating within the Metaverse the corporation's structure and functioning. Then we input the data collected (digital risks and digital preventive measures). The expectation is that matching the data in the Metaverse it could recreate the situational risk of the company and verify if the preventive measures will avoid the commission of corporate crimes.

If the measures contain the risks, the compliance programs should be considered adequate, although a crime would be committed. In fact, in this case, it would mean that someone intentionally circumvented the preventive rules, and he or she should be the only one being punished for the criminal conduct.

Technically, these promises could be challenging to fulfil. In fact, to be trustworthy, the predictive system requires accurate and complete data collection and. It also requires empirical studies and several tests, which we are currently carrying out at the University of Salerno.

Nevertheless, these could be excellent arguments for more studies and development of digital compliance, not a reason to refuse the transition to a digital world.