FINTECH, BLOCKCHAIN AND THE ISSUE OF TRACEABILITY IN FINANCIAL TRANSACTIONS

ELISABETTA PEDERZINI, UNIVERSITÀ DI TRENTO
elisabetta.pederzini@unitn.it

The peculiarities of the *FinTech* system are most closely related to the second term of the contraction, *Tech*, i.e. that connoting in a highly technological sense the financial activities, operations, companies, techniques, and procedures, as well as the financial sectors, subjects, intermediaries, and operators, in its postulation of separate and singular treatment given that 'separate' and 'singular' are the questions posed to the interpreter.

Immediate and priority in the reconstruction of the system - and in the consequential judgment in terms of compliance with the legal principles of a given order or of antinomy in the comparison with certain disciplines - is the reference to the technology shortly referred to as *blockchain*, which the *FinTech* universe crosses and underlies in its multiple manifestations, in order to summarily outline its structural characteristics and operating modes.

The traceability of the financial transactions significantly converges in the many manifestations of *FinTech* and obviously involves both the objective sphere (negotiations and financial services) and the subjective aspect (the contracting parties and customers). Referring to the traceability, crucial questions exist, related to straightforward criminal law as well as to purely private law issues.

On the one hand, the possible violation of the national and supranational rules designed to prevent the use of the financial system and the *cryptocurrencies* for the purpose of money laundering and criminal financing of terrorism and other criminal activities. With specific regard to the European Union, a Fifth Anti-Money Laundering Directive was recently approved as a compendium and modification of previous harmonization measures, as a clear demonstration of the heightened attention paid to a sector crucial for the implementation of the single market and considered to render it particularly vulnerable (EU Directive 2018/843 on the prevention of the use of the financial system for money laundering or financing terrorism). The use of *blockchain* technology allows, with respect to the operations performed, non-retractability and invariability, accurate time stamping, stability, and indelibility of the registered operations once they have occurred. Conversely, with respect to the identification of the subjects, it creates more or less definitive and irreversible forms of opacity and concealment.

On the other hand, the comparison with the protection, processing and circulating of personal data in compliance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (*General Data Protection Regulation – GDPR)*, in force since May 25, 2018. In

particular, the evaluation of the technical-functional characteristics and the structural repercussions in terms of traceability is reversed here and it is antithetical to the reflection on criminal law made earlier. To guarantee the confidentiality of personal data as defined by Art. 4 of the Regulation is, properly speaking, the element that best concretizes the criminal unknown, while the high level of *transparency and immutability* offered by that confidentiality averts the risk of contradicting in an irreversible manner the programmatic power of control over an interested party's personal data and its circulation. In fact, the subjective non-traceability – thus complete *anonymity* of the parties – removes the data referable to them, possibly recorded on platforms or shared through the blocks of the chain, to the very area of application of the Regulation, thus making operations through *blockchain* perfectly compatible, in the abstract, with the strict protection provided for therein. However, the imperishable objective traceability of transactions – along with the distributed nature, the free accessibility, and the transparency of the system – strongly threatens the individual rights to protect their personal data, to control its circulation and to the limit the methods and purposes of its treatment.

The paper suggests that the issue can be faced, if not solved, by exploiting the legal paradigm and the technical methods of *pseudonymisation*.