DOI: 10.5817/MUJLT2017-2-7

STOCK EXCHANGE INTERCONNECTIONS AND LEGAL ISSUES IN DATA EXCHANGE

by

RADIM POLČÁK*

If philosophical cybernetics was interested in stock exchanges, it would probably treat them as relatively simple information structures. From that perspective, stock exchanges can be viewed as places where data on supply and demand of various negotiable instruments are processed. Besides that, stock exchanges, as institutions, provide respective transactions with additional informational (organisational) value that mostly consist of trust regarding the traders, clearing etc.

Consequently, a stock exchange interconnection can be seen as very natural process providing for bigger pool of useful data. One of key tasks in the establishment of exchange schemes is then not to hinder or diminish the added information value, i.e. to at least keep the existing level of trust. In that sense, one of the most important components of interconnection design is the legal compliance.

In the comment, we will examine some of the most emerging legal issues in data sharing between stock exchanges that were subject to examination under recently concluded project 'Creating a legal and regulatory framework for interconnections between stock exchanges: A comparative study of the UK and Taiwan' funded by the British Academy (UK) and the Ministry of Science and Technology, Taiwan. We will particularly focus in this comment on compliance issues in cross-border transfers of personal data and newly emerging regulatory phenomenon of cybersecurity.

KEY WORDS

Stock Exchange, Data Protection, Cybersecurity, Virtualisation

* radim.polcak@law.muni.cz. Head of the Institute of Law and Technology at the Faculty of Law, Masaryk University, The Czech Republic.

1. VIRTUALISED STOCK EXCHANGE

One of must-sees of the Chicago Institute of Art is the original Chicago Stock Exchange Trading Room. The reconstructed creation of Dankmar Adler and Louis Sullivan nicely demonstrates the wealth and style of America's second city at the end of the nineteenth century. It also shows how architectural aesthetics was important for stock exchanges of that time. Good (rich) looking building and trading room was an asset that was for a stock exchange as inevitable as its listing program or trading services.

Times have changed and stock exchange is not defined any more with immovable assets. Today, the CHX does not even mention its building or trading room on its website. It is then reasonable to ask what defines today a stock exchange or more provocatively what defines today a financial market.[1] Subsequently, one might even ask what defines a stock exchange or a financial market not only today but as such.[2]

The reason we always tend to ask these questions in connection to technological developments was earlier described by Pierre Lévy as virtualisation.[3] Lévy demonstrated that technology from time to time allows or even makes us to reshape various societal phenomena. Technologies in that case do not affect the very nature, or core, of those phenomena, but might substantially change their forms. Virtualised money still act as a value-bearer, yet they have, compared to paper money, no tangible form.

It is a bit tricky to treat '*virtual*' as an opposite to '*real*'. Our feelings to '*virtual*' friends are as real as those to '*real*' ones similarly as a value represented by money is supposed to be '*real*' regardless of whether its bearer is tangible or electronic. Thus, virtuality is not the opposite of reality but its another form.[4]

---

[1] Introduction of trust technologies even evokes a question whether financial institutions such as stock exchanges represent defining element of financial markets as such – see for example Reyes, C. L. (2016) Moving Beyond Bitcoin to an Endogenous Theory of Decentralized Ledger Technology Regulation: An Initial Proposal. *Villanova Law Review*, 61, p. 191.

[2] Carran asks a similar question regarding the nature and purpose of stock exchanges and cites the following passage from House of Lords decision in Weinberger v Inglis [1919] A.C. 606, HL 1: '*The London Stock Exchange is in reality a building vested in certain proprietors and used for the purpose of carrying on a market for stocks and shares*.' See Caran, P. C. (1975 –1978) Some Aspects of the Stock Exchange: Its Nature and Functions. *Victoria University Wellington Law Review,* 8, p. 71.

[3] See Lévy, P. (2002) *Becoming Virtual – Reality in the Digital Age.* New York: Plenum Trade.

[4] See Lévy, P. (1997) Welcome to virtuality. *Digital Creativity*, 8(1), p. 3.

Virtualisation causes some old problems to disappear, while new ones instantly pop up.[5] It is typical that namely problems associated with physical place (or placement) entirely vanish, because virtualisation is normally accompanied with loss of substance (or tangibility). On the contrary, new problems of virtualised phenomena are typically linked with various technology risks. A success of virtualisation can be called a situation when those problems that fell off had been worse than those that newly emerged – which means that not all societal phenomena are fit for virtualisation all the time.

It is also important to properly distinguish between mere substantive core and formal elements to master the virtualisation of some phenomenon, let it be friendship, money, justice or anything else. The identification of the core can provide for a protection of respective phenomenon from substantive erosion.[6] At the same time, properly knowing which elements of virtualised phenomenon are just formal enables us to maximise various positive effects of virtualisation, prevent unnecessary defects and prepare for necessary ones.[7]

The fact that we see today the original Chicago Stock Exchange Trading Room as a gallery object and that it was not replaced at the CHX by anything even architecturally or aesthetically fancier shows that stock exchanges simply got virtualised in past decades. It is then not only thanks to the use of ICT that trading rooms (i.e. physical locations where trade deals are made) do not represent core facilities of stock exchanges any more, but thanks to natural tendency of stock exchanges to develop further and to liberate trading from various obstacles. In this case, virtualisation was probably quite successful, because the problems lost (i.e. direct dependence of trading on physical presence of traders on the floor of the trading room) seem to be more serious than those that newly emerged (incl. the loss of aesthetic amusement of traders).[8]

---

[5] For a detailed study regarding particular virtualisation of financial markets, see Chiu, I. H-Y. (2016) *Journal of Technology Law & Policy*, 21, p. 55.

[6] When Trautman and Harell discuss the use of bitcoin technology for financial transactions, they start with the question as '*what is money*'. See Trautmann, L. J., Harell, A. C. (2017) Bitcoin Versus Regulated Payment Systems: What Gives? *Cardozo Law Review*, 38, p. 1041.

[7] See for example Batog, C. Blockchain: A Proposal to Reform High Frequency Trading Regulation. *Cardozo Arts & Entertainment Law Journal*, 33, p. 739.

[8] See for example Engelen, P.-J. (2006) Changes in the Securities Trading Landscape in Europe and the U.S. *Competition and Regulation in Network Industries*, 1, p. 439.

The example of the CHX also demonstrates that neither architectural aesthetics nor physical presence of traders represent core elements of the phenomenon of a stock exchange. Both these features were already almost entirely lost with the introduction of ICT, but the stock exchange still exists and operates as a stock exchange.

2. INTERCONNECTIONS AS MEANS OF STOCK EXCHANGE VIRTUALISATION

Stock exchange interconnections[9] represent yet another way of virtualisation of stock exchanges. Interconnections are possible thanks to ICT and their purpose is to make further use of already present dematerialisation of stock trading. Similar with the shift from physical to virtual trading rooms, interconnections bring a shift from trading at multiple hubs to trading at one place. While virtualisation of a trading room introduced a possibility to trade between members who are not physically present at one place (in the trading room), interconnections make possible trading stock that is not available on local market.[10]

We noted above that virtualisation of any kind can be successful only if we get right the fundaments of respective phenomenon. Only then we can make proper use of its positive effects and successfully tackle in sufficient advance newly emerging problems.

Every stock exchange can be viewed from the perspective of information theory as a system that processes data. Stock exchange receives input data about offer and demand and turns them into information by adding an extra value to them and matching them together. Particularly, stock exchanges provide for concentrated and structured access to respective data (offer and demand incl. accompanying data) and they also increase informational value of that data by business trust related to offered stock and consequent clearance.[11] From that perspective, traders pay stock exchanges for extra value that consists primarily of efficient access to stock market (from both sides) and transactional credibility.

---

[9] The phenomenon of stock Exchange interconnections was recently examined in a project funded by the British Academy (UK) and the Ministry of Science and Technology of Taiwan and titled: Creating a legal and regulatory framework for interconnections between stock exchanges: A comparative study of the UK and Taiwan. Further findings presented in this paper are primarily based on research undertaken within that project.

[10] Interconnections thus bring significantly different effects in comparison with mergers – see for example Kokkoris, I. and Olivares-Caminal, R. (2007–2008) Some Issues on Cross-Border Stock Exchange Mergers, *University of Pennsylvania Journal of International Law*, 29(2), p. 455.

Any virtualisation, if it is to do no harm to primary functions of stock exchanges, must preserve the aforesaid way in which stock exchanges turn data into information. Interconnections bring the opportunity for more data (on supply and demand side) to enter the stock exchange. One kind of risk then arises from different compliance standards of data that are being exchanged through the interconnection. Apart general stock regulatory issues (i.e. differences between stock market regulations in different jurisdictions), we must tackle issues related to data rights compliance (e.g. there are *sui generis* rights to databases in the EU, while no such rights exist anywhere else in the world).

The second type of legally relevant risks with regards to data that arise from stock exchange interconnections relate to security. Stock exchanges have always been extremely cautious about data security, because any breaches can seriously harm their reputation. Data security issues can also hugely affect one of aforesaid reasons for which traders use stock exchanges, i.e. transactional trust. Thus, substantive information systems of stock exchanges are highly secured which also means they are isolated from the rest of the internet to maximum possible extent.

Interconnection always means opening the information system and exposing it to external sources of data. Apart the aforesaid problem of differences in substantive standards between stock markets (incl. legal compliance), there is substantial increase of risk caused by distant communication. Stock exchanges can never be directly connected, so there is always a need for an information intermediary (e.g. a telecommunications provider).

While geographic distance is relevant as such (i.e. it represents a risk factor), there is no direct correlation between the distance and the possibility of stock exchange interconnections. Other sorts of trade relations between different nations often depend, for obvious reasons, on geographic proximity. As data can travel at any distance, there is no practical difference in establishment of stock exchange interconnections between any places in the world. In other words, once the above issues are

[11] This function of stock exchanges may partly vanish in near future with the introduction of technologies that will provide for trusted authentication and confidentiality – see for example Lee, L. (2017) New Kids on the Blockchain: How Bitcoin's Technology Could Reinvent the Stock Market, *Hastings Business Law Journal*, 12, p. 81, or Walch, A. (2015), *N.Y.U. Journal of Legislation and Public Policy*, 18, p. 837.

sorted, physical distance does not have to play any role in deciding about which stock exchanges are to be connected.

3. PERSONAL DATA

The scope of the definition of personal data is rather broad, namely thanks to the criterion of '*identifiability*'. It is under permanent discussion of legal academics across Europe whether the meaning of '*identifiability*' is in this case subjective or objective, i.e. whether a controller shall obey the rules upon the data being subjectively identifiable by that controller or objectively (theoretically).[12]

The Court of Justice of the EU recently ruled for the subjective interpretation that is slightly more restrictive (the court ruled that an internet service provider is considered a controller of personal data if it

> *"has the legal means which enable it to identify the data subject with additional data which the internet service provider has about that person"*[13]).

However, the court still upheld earlier rather extensive approach to the question as to which data are to be considered identifiable by stating that even a dynamic IP addresses can be identifiable in the sense of Art. 2(a) of the Directive 95/46/EC.

Although the subjective interpretation of the definition of personal data slightly limits the scope of application of data protection rules, that limitation hardly applies to stock exchanges. Despite some personal data that are regularly communicated through interconnections might be anonymised or pseudonymised, stock exchanges still hold means for reverse identification of particular individuals (incl. measures arising from AML obligations or KYC procedures).

In result, stock exchange interconnections inevitably include communications (exchange) of personal data within the meaning of Art. 2(a) of the Directive 95/46/EC. It implies that whenever an interconnection is made between a stock exchange within and outside the EU (or EEA), the data processing must comply with EU rules

[12] See for example Oostveen, M. (2016) Identifiability and the Applicability of Data Protection to Big Data, *International Data Privacy Law*, 6(4), p. 299.

[13] See Case-C-582/14 Patrick Breyer v. Bundesrepublik Deutschland.

for personal data transfers or even directly with extraterritorially applicable substantive rules for processing of personal data within the EU.[14]

Offshore data transfers recently represented quite turbulent agenda around the EU and it is still not entirely clear which instruments will provide desired essential equivalence under the GDPR.[15] Despite all contemporary problems and uncertainties in EU data protection laws, the prospect for stock exchange interconnections is relatively optimistic.

The reasons for our optimism were mostly institutional. Stock exchanges are equipped with state-of-the-art data security measures and compliance procedures. That allows them to relatively easily develop and maintain binding corporate rules as envisaged by Art. 47 of the GDPR or similar instruments that require approval by the respective data protection authority. If stock exchange interconnections become popular, it is even possible to think about adopting specific certification schemes or developing standard contractual clauses that would be adopted into interconnection agreements. In addition, the economic relevance of stock exchanges often allows them to actively influence domestic or foreign policing which might lead even e.g. to the conclusion of international agreements laid down in Art. 46(2)(a) or Art. 46(3)(b). In any case, it is advisable for interconnecting stock exchanges to invest into the development of proper personal data transfer compliance mechanisms rather than to argue that data protection or data transfer rules do not apply here.

4. CYBERSECURITY

Stock exchange interconnections obviously require establishment of proper means of communication and data storage. As data represent absolutely essential asset for stock exchanges, there is no space for half-way solutions or compromises. From security standpoint, it would be ideal if substantive information systems used by stock exchanges would be entirely independent on the Internet. That option, however, is not possible as it would prevent the availability of a number of popular trading services. Consequently, stock exchanges must tackle same security problems as those

[14] See for example De Hert, P., Czerniawski, M. Expanding the European Data Protection Scope Beyond Territory: Article 3 of the General Data Protection Regulation in its Wider Context, *International Data Privacy Law*, 6(3), p. 230.

[15] See for example Bender, D. (2016) Having Mishandled Safe Harbor, Will the CJEU do Better with Privacy Shield? A US perspective, *International Data Privacy Law*, 6(2), p. 117.

that arise in any systems connected to the Internet. Interconnections then only extend the scope and placement range of information assets that need to be secured.

Cybersecurity recently became also a regulatory issue in the EU. The NIS Directive[16] now brings entirely new compliance regime into the national laws of the member states. Stock exchanges fall within the scope of the NIS Directive which means that member states include them into the count of institutions whose systems are obliged to meet national security standards incl. an obligation to report security incidents to national response teams.

Compliance duties that are or shortly will be laid down in the laws of the member states upon the NIS Directive[17] do not obstruct stock exchange interconnections. They only require stock exchanges to build technical means for interconnections under same security standards and cover them with same operational duties as the rest of their information and communication infrastructures.[18]

At first, we do not expect any serious problems regarding technical compliance of stock exchanges with security standards that are or will be laid down in EU member states. Most financial institutions incl. banks, stock exchanges, insurance and reinsurance companies etc. already have in place strong cybersecurity measures that comfortably meet or often exceed new legal requirements. Thus, we might expect that only attention will mostly have to be paid to organisational adoption of existing cybersecurity measures to new security standards, documentation and establishment of incident reporting functionalities.

It might become problematic for establishing technically and legally functioning interconnection between stock exchanges namely if cybersecurity standards laid down in respective countries substantially differ. In that case, there will be a need for the development of technical and/or organisational security interface that would properly incorporate the interconnection into compliance structures on both sides.[19]

---

[16] See Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

[17] The Directive shall be legislatively implemented by the member states by 9 May 2018.

[18] Interconnections infrastructures fall within class 4 (Financial market infrastructures) according to Annex II of the NIS Directive.

[19] NIS Directive does not provide for any equivalence regime, so compliance has to be tackled specifically within and outside the EU.

Not legally required but highly advisable for contractual framework of interconnections are measures for mutual sharing of data on cybersecurity incidents between interconnected stock exchanges.[20] If these security data are shared, it can provide for higher level of mutual credibility. In addition, it can also increase the probability of detecting serious incidents on both sides and improve consequent response capabilities.

Data on cybersecurity incidents are not important only for stock exchanges as such. Regulators of various capital markets also require listed companies to report significant cybersecurity incidents that occurred in their infrastructures. The reason is that cybersecurity incidents might directly affect operations of listed companies and influence the value of their shares.[21] It then hugely depends on particular details of such reporting obligations of listed companies, namely on types of compulsorily reported incidents, structure of reports or timeframes, but there is no doubt these data do not just have value for investors, but they might also give a very good picture about security situation in respective country.

If cybersecurity data of listed companies are subject to data exchange within stock exchange interconnection, they might become, one way or another, transparent to security institutions in respective foreign country. That can represent serious concern for national security. On the contrary, a stock exchange interconnection can be even utilised by security institutions on both sides, because it can provide them with a mutually secure channel through which they can get potentially valuable cybersecurity data from another country including sophisticated analytics.[22] Thus, the availability of cybersecurity data about listed companies through stock exchange interconnections can represent security risk or security asset, depending on how respective security institutions are able to cooperate with participating stock exchanges (it is needless to add here that we do not expect stock exchange interconnections to be established between countries with substantially diverse security interests).

---

[20] These might include exchange of periodic security reports or even real-time exchange of incident reporting and/or incident management data between incident response teams on both sides. There already exist numerous technologies for such data sharing, e.g. the IODEF or IDMEF data formats.

[21] See for example Bledstein, N. (2013) Is Cyber Espionage a Form of Market Manipulation. *Journal of Law & Cyber Warfare*, 2(1), p. 104.

[22] For more detailed description of international cooperation schemes in cybersecurity, see for example Gross, O. (2015) Cyber Responsibility to Protect: Legal Obligations of States Directly Affected by Cyber-Incidents, *Cornell International Law Journal*, 48, p. 481.

5. CONCLUDING REMARKS

Cybersecurity and protection of personal data do not represent only data--related legal issues of stock exchange interconnections. Legal framework for interconnection of stock exchanges out of which at least one is in the EU has always to tackle other issues such as *sui generis* rights to databases, anti--money laundering reporting obligations etc. In addition, international interconnections are always burdened with general questions of contemporary cyberlaw such as delimitation of state jurisdictions, liability of information society service providers, competence conflicts of regulators (financial markets, telecommunications, competition)[23] etc. However, none of these issues is fatal for establishment or functioning of stock exchange interconnections as such.

Even the Brexit does not represent with regards to data-related laws any serious obstacle or source of fatal uncertainties for further development of interconnection projects between stock exchanges in the UK and those in other EU member states or elsewhere. It is now mostly clear that UK is about to keep the existing EU legal regulatory framework for data processing and cybersecurity, so interconnections can be further developed according to the existing EU regulatory standards.[24]

Consequently, the conclusions with regards to rights related to data are rather positive. Instead of general or fatal obstacles we found only particular regulatory issues that can be resolved mostly through diligent compliance mechanisms.

LIST OF REFERENCES

[1] Batog, C. Blockchain (2015) A Proposal to Reform High Frequency Trading Regulation. *Cardozo Arts & Entertainment Law Journal*, 33, p. 739.

[2] Bender, D. (2016) Having Mishandled Safe Harbor, Will the CJEU do Better with Privacy Shield? A US perspective. *International Data Privacy Law*, 6(2), p. 117.

[3] Bledstein, N. (2013) Is Cyber Espionage a Form of Market Manipulation. *Journal of Law & Cyber Warfare*, 2(1), p. 104.

[4] Case C-582/14 *Patrick Breyer v. Bundesrepublik Deutschland*, ECLI:EU:C:2016:779.

[23] See the debate between Tamar Frankel and Omri Yadlin in Chicago–Kent Law Review: Frankel, T. (1998) The Internet, Securities Regulation, and Theory of Law. *Chicago–Kent Law Review*, 73, p. 1319 and Yadlin, O. Should the Sec Regulate the Cybersecurities Market? *Chicago–Kent Law Review*, 73, p. 1355.

[24] See McCullagh, K. (2017) Brexit: Potential Trade and Data implications for Digital and 'fintech' Industries, *International Data Privacy Law*, 7(1), p. 3.

[5] Caran, P. C. (1975-1978) Some Aspects of the Stock Exchange: Its Nature and Functions. *Victoria University Wellington Law Review*, 8, p. 71.

[6] Chiu, I. H-Y. (2016) Fintech and Disruptive Business Models in Financial Products, Intermediation and Markets – Policy Implications for Financial Regulators. *Journal of Technology Law & Policy*, 21, p. 55.

[7] De Hert, P., Czerniawski, M. (2016) Expanding the European Data Protection Scope Beyond Territory: Article 3 of the General Data Protection Regulation in its Wider Context. *International Data Privacy Law*, 6(3), p. 230.

[8] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 31995L0046, OJ L 281, 23. 11. 1995, p. 31–50 .

[9] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, 32016L1148, OJ L 194, 19.7.2016, p. 1–30.

[10] Engelen, P.-J. (2006) Changes in the Securities Trading Landscape in Europe and the U.S. *Competition and Regulation in Network Industries*, 1, p. 439.

[11] Frankel, T. (1998) The Internet, Securities Regulation, and Theory of Law. *Chicago–Kent Law Review*, 73, p. 1319.

[12] Gross, O. (2015) Cyber Responsibility to Protect: Legal Obligations of States Directly Affected by Cyber-Incidents. *Cornell International Law Journal*, 48, p. 481.

[13] Kokkoris, I. and Olivares-Caminal, R. (2007-2008) Some Issues on Cross-Border Stock Exchange Mergers. *University of Pennsylvania Journal of International Law*, 29(2), p. 455.

[14] Lee, L. (2017) New Kids on the Blockchain: How Bitcoin's Technology Could Reinvent the Stock Market. *Hastings Business Law Journal*, 12, p. 81.

[15] Lévy, P. (1997) Welcome to virtuality. *Digital Creativity*, 8(1), p. 3.

[16] Lévy, P. (2002) *Becoming Virtual – Reality in the Digital Age*. New York: Plenum Trade.

[17] McCullagh, K. (2017) Brexit: Potential Trade and Data implications for Digital and 'fintech' Industries. *International Data Privacy Law*, 7(1), p. 3.

[18] Oostveen, M. (2016) Identifiability and the Applicability of Data Protection to Big Data. *International Data Privacy Law*, 6(4), p. 299.

[19] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 32016R0679, OJ L 119, 4.5.2016, p. 1–88.

[20] Reyes, C. L. (2016) Moving Beyond Bitcoin to an Endogenous Theory of Decentralized Ledger Technology Regulation: An Initial Proposal. *Villanova Law Review*, 61, p. 191.

[21] Trautmann, L. J., Harell, A. C. (2017) Bitcoin Versus Regulated Payment Systems: What Gives? *Cardozo Law Review*, 38, p. 1041.

[22] Walch, A. (2015) The Bitcoin Blockchain as Financial Market Infrastructure: A Consideration of Operational Risk. *N.Y.U. Journal of Legislation and Public Policy*, 18, p. 837.

[23] Yadlin, O. Should the Sec Regulate the Cybersecurities Market? *Chicago–Kent Law Review*, 73, p. 1355.