

JOANNA PTAK

JAGIELLONIAN UNIVERSITY
FACULTY OF LAW AND PUBLIC ADMINISTRATION
DEPARTMENT OF SOCIOLOGY OF LAW
E-MAIL: JOANNA.PTAK@DOCTORAL.UJ.EDU.PL

Social Network Analysis, Crime Prevention and Human Rights

ABSTRACT

Use of Social Network Analysis (hereinafter as SNA) in crime prevention and law enforcement is widely discussed from either practical or theoretical point of view. Although its advantages are commonly acknowledged, incorporation of SNA into strategies of combating crime raises various controversies. The main aim of this paper is to present risks connected with application of SNA in practice, as a part of policing, from the point of view of the human rights system. The assumption is that all of legal responses to violence have to be in accordance with the human rights law requirements. As this subject matter is exceptionally complex, two main aspects of this issue have been chosen on the base of their significance – risk of infringement of the right to privacy and of politicization of the use of SNA, especially in the context of so-called “suspect communities.” The possibility of indication of prompt solutions to presented matters has been discussed. As such, this paper is an introduction to presented subject area and provides a basis for further research.

KEYWORDS

social network analysis, SNA, human rights, law enforcement, crime prevention, pre-crime

Introduction

In the most general form, the subject matter of Social Network Analysis (hereinafter as SNA) are social relations, visualized with the use of points (as the reflections of individuals or groups, dependent on a research purpose) and lines (as the symbol of various relations between particular points). The mathematical graph theory is used to present the network,

therefore SNA is more dimensional than pure link analysis. The concept that stands behind the SNA is that the mutual relations and connections between groups of individuals or collectives reflect the model of structures within that group, for example showing the hierarchy or the potential social role of the particular entity. However, even though the history of use of SNA as a research technique dates back to the early 1970s,¹ its usefulness as a tool of criminal prevention is still a subject of an ongoing and heated debate.

Arguments in favor of the use of SNA in prevention of crimes refer to its effectiveness due to the multitude of information that SNA may provide to the researcher, starting from such data as the hierarchy within the network, the impact of the network on an individual, and its role as a risk factor of the commission of crime. What is more, due to its universal character, SNA may be used in evidence-based policy making in reference to public policies of combating various kinds of crime, for example terrorism, gang violence, drug dealing and human trafficking. Last but not least, as research has shown, SNA may be used to predict the probability of the victimization regarding such types of crimes as gun violence.²

On the other hand, use of SNA in law enforcement rises various controversies. First of all, effective use of this research technique requires gathering of information that may be considered as sensitive and infringing the right to privacy. Another issue is connected with boundaries of exchange of information between various state agencies in order to improve the efficiency of analysis of particular network. What is noteworthy, improperly applied SNA can be used as a tool of political games, either intentionally or unconsciously.

Due to the rising popularity of SNA, recognition of rules of its proper application and rising the awareness of its potential risks are exceptionally important and should be widely discussed as a subject of scientific debate. Taking it into consideration, the main aim of this article is to present risks connected with the use of SNA as a tool of law enforcement and prevention of crimes from the point of view of the human rights system. Deliberations included in this paper are at an abstract level, without focusing on any particular example of a social network. The assumption is that legal responses to violence have to incorporate human rights law and its principles. Due to

¹ For the historical roots and the development of SNA read: J. Scott, *What is Social Network Analysis?*, London–New York 2010.

² A. Papachristos, Ch. Wildeman, E. Roberto, *Tragic, But Not Random: The Social Contagion of Nonfatal Gunshot Injuries*, "Social Science & Medicine" 2015, Vol. 125, pp. 139–150.

complexity of this problem, the scope of the paper is limited to issues that were selected on the basis of their importance and significance to proper presentation of subject matter and as such, it provides a basis for further research. All of those issues are, either directly or indirectly, connected with one particular question – about sources and boundaries of data collection for SNA purposes.

SNA and human rights

The use of SNA as a tool of crime prevention is discussed either in reference to criminological research or in the process of law enforcement. One of the requirements of lawful prevention of crimes is the incorporation of the human rights system into it. The importance of placing legal responses to violence within the framework of the human rights system requirements was stressed by the United Nations in various documents,³ in reference to all types of crimes, including those that are the subject of interest of researchers using SNA, such as terrorism or drug dealing.

When it comes to SNA, the risk of infringement of human rights of people placed within the social network is noticeable. This risk is complex and refers to various rights. One of them is the right to privacy, which will be discussed in details in the next part of this article.

a. The right to privacy. Usefulness of SNA as a tool of crime prevention

Among the most controversial issues connected with the use of SNA by law enforcement agencies one may find the problem of sensitivity of information gathered by researchers and/or law enforcement agencies especially important. Lines that connect nodes of graphs may refer to various relationships, such as co-offending, friendship, romance, exchange of information. What is more, gained information may be collected with the use of many different means, for example through collecting of private data from phone calls, police statistics, or surveillance of the online activity. Use of some of those means, such as the analysis of official police statistics, are less contro-

³ For example: Article 11 of *United Nations Declaration on Crime and Public Security*, Resolution of General Assembly number A/51/610, [online] <http://www.un.org/documents/ga/res/51/ares51-60.htm> [accessed: 01.03.2017] or in *The United Nations Global Counter-Terrorism Strategy Review*, Resolution of the General Assembly of UN number 70/9, [online] http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/70/291 [accessed: 1.04.2017].

versial than others. From the point of view of “innocent until proven guilty,” use of information that was already acquired during investigations led by police forces and marked as criminal activity differs from wiretapping of private phone calls in search for a potential wrongdoing.

However, independently on the source of information, use of those techniques is unavoidably connected with the risk of infringement of the right to privacy. This right, as a part of the human rights system, is incorporated – *inter alia* – in Article 12 of the Universal Declaration of Human Rights,⁴ according to which “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.”⁵ The aforementioned example of wiretapping of private phone calls in search for signs of potential criminal activity is a severe interference with one’s privacy at its core.

Eventual lawfulness of such interference depends on various factors, such as necessity of applied solutions and lack of arbitrariness. To elaborate on that, “the introduction of the concept of arbitrariness is intended to guarantee that even interference provided for by the law should be in accordance with the provisions, aims and objectives of the Covenant⁶ and should be, in any event, reasonable in the circumstances.”⁷ By “reasonableness” one shall understand that “any interference with privacy must be proportional to the end sought and be necessary in the circumstances of any given case.”⁸

If so, to sum up at this point, lawful use of collection of data for SNA, for example in the form of wiretapping, in reference to the right to privacy should meet such requirements as: (1) necessity of use of this technique to achieve legitimate aim, (2) proportionality, (3) legal base of application of SNA. What is more, it should be the least invasive option from those available.⁹

Taking this list into consideration, it is crucial to discuss first and foremost the usefulness of SNA as a tool of achieving legitimate aims. In other words, in reference to the subject topic of this article, it has to be deter-

⁴ The Universal Declaration of Human Rights, [online] <http://www.un.org/en/universal-declaration-human-rights/index.html> [accessed: 1.04.2017].

⁵ *Ibidem*.

⁶ International Covenant on Civil and Political Rights.

⁷ Human Rights Committee, General Comment 16, 23 session, 1988, [online] <http://hrlibrary.umn.edu/gencomm/hrcom16.htm> [accessed: 1.04.2017].

⁸ Communication Number 488/1992 of Human Rights Committee, *Toonen v. Australia*, [online] <http://hrlibrary.umn.edu/undocs/html/vws488.htm> [accessed: 1.04.2017].

⁹ *The right to privacy in the digital age, Report of the Office of the United Nations High Commissioner for Human Rights*, 30th of June 2014, p. 8.

mined if the use of SNA may result in the reduction of crime rates as a tool of effective crime prevention.

On the base of preliminary research, it seems that the answer is positive. As various research has shown, analysis of social networks enables, among others, to evaluate the risk of gunshot victimization,¹⁰ to discover the patterns of gang violence,¹¹ to predict leadership roles within criminal organizations,¹² to identify structures of criminal networks and their changes over time,¹³ and to gain knowledge about the structure of drug trafficking groups.¹⁴ However, the most significant advantage, connected with application of SNA, is that considering the multiplicity of information it may deliver to a researcher it is more effective as a tool of gaining scientific knowledge about crime patterns than other methods and techniques that are used in studies of crime.

The example of such techniques is link analysis. What primarily differentiates link analysis and SNA is the use of mathematical calculation that enables analysis of not only links between actors (nodes of the graph), without focusing on additional information, but also of mechanisms of creation of the network, its structure and changes over time. In the case of SNA observation and visualization of relations between nodes is rather a tool of further research than the goal *per se*.

When it comes to further points of the list, the requirements of proportionality and legal base of use of SNA, their fulfilment depends on circumstances of a particular case. To exemplify it, on the base of preliminary research it may be noticed that due to its features SNA is particularly useful as a tool of crime prevention and law enforcement in relation to organized crime. Taking it into consideration, use of SNA with the aim of preventing organized crime, such as terrorist nets, would be proportional and legitimated, if its application was adequate to severity of the crime itself and based on the legal rule.

¹⁰ A. Papachristos, Ch. Wildeman, E. Roberto, op. cit., pp. 139–150.

¹¹ A. Papachristos, D. Hureau, A. Braga, *The Corner and the Crew: The Influence of Geography and Social Networks on Gang Violence*, "American Sociological Review" 2013, Vol. 78, Issue 3, pp. 417–447.

¹² G. Berlusconi, *Social Network Analysis and Crime Prevention*, [in:] *Crime Prevention in the 21st Century. Insightful Approaches for Crime Prevention Initiatives*, eds. B. LeClerc, E. Savona, Cham 2017, pp. 129–141.

¹³ Ibidem.

¹⁴ F. Calderoni, *The Structure of Drug Trafficking Mafias: the 'Ndrangheta and Cocaine*, "Crime, Law and Social Change" 2012, Vol. 58, Issue 3, pp. 321–349.

Mentioned example refers to states' counter-terrorism strategies. Prevention of crimes falling into the category of "terrorism" differs from other types of crime. One of such differences is connected with widely approved allowance of use of pre-crime as a part of counter-terrorism strategy, which will be discussed later.

This allowance is caused by the particular severity of terrorist activity. In fact all of types of organized crime have features that justify state's extensive interest in their prevention, such as a multidimensional covertness or involvement of many individuals in the criminal activity. If so, use of more infringing methods and techniques, such as SNA, seems to be justified as proportional to severity of the crime and necessary to achieve legitimate purposes. However, in spite of those particularities of organized crime, as it was mentioned earlier, detailed evaluation of proportionality and legal base of use of SNA requires analysis of features of each of cases.

Last but not least, when it comes to the issue of invasiveness of SNA, interference into the sphere of privacy of those involved in a particular social network is the core of this technique. However, as it is applied mostly to those crimes that are based on covertness, hierarchy, social organization and fulfillment of particular roles by members of criminal groups, such interference is unavoidable to gain knowledge about the structure of the group, its size, or geographical range. Information about those features is crucial to ensure effective crime prevention. If so, if other requirements of avoidance of violation of the right to privacy are met, application of SNA should be allowed.

Significantly, to give another example, further potential problem concerning privacy and SNA is the issue of exchange of information between various public institutions and state officers, working within the field of law enforcement. Christopher Yang and Xuning Tang argue that such exchange of knowledge would make SNA more effective.¹⁵ They assume that creating a complete social network analysis would require collecting all the information stored by the law enforcement and other agencies and institutions working in area of crime-prevention. Otherwise any SNA would be just partial.¹⁶ The issue of such exchange raises various problems with finding a balance between violation of the right to privacy and the utility of shared in-

¹⁵ Ch. Yang, X. Tang, *Information Integration for Terrorist or Criminal Social Networks*, [in:] *Security Informatics. Outlines the Foundations and Parameters of the Field of Intelligence and Security Informatics (ISIS)*, eds. C. Yang, M. Chau, J.-H. Wang, H. Chen, Springer 2010, pp. 41–57.

¹⁶ *Ibidem*, p. 42.

formation. Since anonymized SNA is no longer fully functional, any anonymization of data affects its effectiveness as a tool of law enforcement. Detailed evaluation of Yang's and Tang's proposition of practical solution to this problem – sub-graph generalization approach – is out of the scope of this paper, but the important conclusion that comes from the analysis of their work is that in reference to law enforcement and activity of state officers, application of SNA is connected with the risk of infringement of the right to privacy at multidimensional level.

b. SNA and the risk of politicization

Another risk, connected with what was discussed before as an issue of variety of sources of data and the infringement of the right to privacy, is a potential creation of so-called “suspect communities” at the pre-crime level and its further consequences.

An idea of pre-crime as paradigm of crime prevention is not new, as it was known before the XXI century.¹⁷ However, its rising popularity dates back to 9/11¹⁸ and the rise of counter-terrorism strategies. Jude McCulloch and Sharon Pickering argue that from the point of view of criminology pre-crime is not a measure of crime prevention.¹⁹ They assume that in general, in the criminological sense crime prevention is based on the non-punitive solutions that refer to, *inter alia*, reduction of opportunities of crime commission with reference to the broader social context. Taking it into consideration, McCulloch and Pickering highlight that “counter-terrorism pre-crime measures envisage specific serious harms and criminalize those whom it is believed will commit these imaginary future harms, while ignoring broader social and environmental factors.”²⁰ To elaborate on that, pre-crime measures in their most controversial form are connected with the use of state force without factual commission of crime; sole suspicion is sufficient.

Even though such activity does not fit into criminological category of crime prevention, it has been used as a tool of law enforcement, especially in reference to counter-terrorism strategies. Mentioned authors argue that this is caused by the fact that proscribing an individual or an organization

¹⁷ For example: L. Zedner, *The Pursuit of Security*, [in:] *Crime, Risk and Insecurity: Law and Order in Everyday Life and Political Discourse*, eds. T. Hope, R. Sparks, New York 2000, pp. 200–214.

¹⁸ J. McCulloch, S. Pickering, *Pre-crime and Counter-terrorism. Imagining Future Crime in the 'War on Terror'*, “The British Journal of Criminology” 2009, Issue 49, p. 629.

¹⁹ *Ibidem*.

²⁰ *Ibidem*.

as “terrorist” is purely a political decision and does not require a confirmation of crime commission in the form of the court verdict.²¹

This issue is strictly connected with the topic of this article. The main assumption that underpins pre-crime in counter-terrorism strategies is that due to the fact that terrorists’ aim is to create mass casualties, they should be stopped from acting prior to their criminal activity in order to reduce human cost.²² From this point of view, SNA may be a useful tool of counter-terrorism, as its outcome is – for example – an understanding of structures of criminal organization and the role of the leaders, or raising the knowledge about the size of the group and its geographical range. In consequence, SNA enables disruption and other forms of action directed against a particular organization.

However, this is just one side of the coin. Due to the fact that labelling an organization as terrorist is rather a political than judicial decision, use of SNA in counter-terrorism is unavoidably connected with the risk of its politicization with all of its further consequences.²³

To elaborate on that, the term “politicization” refers to various processes of making an issue political as a subject of interest of political agencies. In this context it is possible that through the lenses of counter-terrorism strategies SNA would be used against particular groups that had been considered as politically undesirable as the so-called “suspect communities.” This raises the already mentioned question about the boundaries of data collection for SNA purposes.

According to the Universal Declaration of Human Rights, “everyone is entitled to all the rights and freedoms set forth in this Declaration, without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.”²⁴ What is more, when it comes to the example of counter-terrorism strategies, the UN highlights that “terrorism and violent extremism as and when conducive to terrorism cannot and should not be associated with any religion, nationality, civilization or ethnic group.”²⁵ If so, creation of notion about existence of such phenomenon as “suspect community” and, as its further consequence, basing a selection of individuals or groups as a subject matter of SNA on particular ethnic or religious background would be a serious violation of the system of human rights.

²¹ Ibidem, p. 630.

²² Ibidem, p. 632.

²³ This issue will be explained later with the example of Kurds in the United Kingdom.

²⁴ Article 2 of the Universal Declaration of Human Rights.

²⁵ The Resolution of the General Assembly of UN number 70/91, op. cit.

The presented issue is not only hypothetical. Vicki Sentas argues that due to listing of PKK²⁶ as a terrorist organization, Kurds and people of Kurdish origin are regarded as the “suspect community” by security policies.²⁷ Although her qualitative research is limited to the small sample and placed within particular geographical region, it presents various risks connected with criminalization on the base of ethnicity or nationality.

The example of Kurds has been chosen to present this issue, as it is particularly interesting from the point of view of this article. Labelling of Kurds’ self-determination attempts as terrorist is widely discussed.²⁸ Due to the fact that PKK has been listed as terrorist organization in the United Kingdom, counter-terrorism strategies in reference to this entity require designation of boundaries between legal (not connected to PKK) and illegal (connected to PKK) activity. Sentas’ research has shown that the authority to make a decision about “legality” or “illegality” of an act belonged to British policing organs. One of the conclusions of Sentas’ research is that “interviewees believed that their ‘legitimate’ Kurdish rights were being criminalized simply because they supported the political goals of the PKK.”²⁹ What is more, participants of the research considered that disruption strategies affected them due to their ethnicity, not terrorist activity, and were an effect of collective attribution of criminal tendencies to all of Kurds.

The presented example raises questions about the ontological core of counter-terrorism strategies, reflected in a shift to criminalization because of “being” instead of “doing.” In reference to use of SNA in crime prevention and law enforcement, this risk is particularly significant. As it was mentioned, effective use of SNA requires data from various sources. SNA reflects multiple relations, not restricted solely to “pure” criminal activity. If so, the risk of application of this technique to social network because of its ethnicity or religion, instead of criminal activity, is particularly serious and may affect multiple members of vulnerable groups.

When it comes to solution to this problem, contrary to previously described issue, in this case I find it impossible to list in details prerequisites of avoidance of violation of human rights. Criminalization because of “being” instead of “doing” is a matter of application of particular public policies. If so, it is important to be aware of such risk, and its unlawfulness because of

²⁶ Kurdistan Workers’ Party.

²⁷ V. Sentas, *Policing the Diaspora: Kurdish Londoners, Mi5 and the Proscription of Terrorist Organizations in the United Kingdom*, “The British Journal of Criminology” 2016, Vol. 56, pp. 898–918.

²⁸ In relation to the United Kingdom see: *ibidem*, p. 903.

²⁹ *Ibidem*, p. 907.

infringement of human rights, at the level of policy shaping and in the process of its further implementation.

Summary

To sum up, use of SNA as a technique of crime prevention and law enforcement has its advantages and drawbacks. Main benefits from its use are connected with its universality and the multitude of information it may provide to researchers. Due to those features, SNA is particularly useful in reference to those types of crimes that are based on strict organization of human activity and indication of particular roles to be fulfilled by those who are involved in them. As such, social network analysis seem to be a crucial element of evidence-based policy making in reference to, as an example, terrorism, gang violence, drug dealing, or human trafficking.

On the other hand, application of SNA raises various controversial issues. The scope of this article was limited only to those aspects of disadvantages of SNA that were related to – either directly or indirectly – sources and boundaries of data collection for SNA purposes. As it was presented, use of SNA in reference to subject matter of this article is connected with the risk of infringement of various human rights. One of them is the right to privacy, which may be violated at multidimensional level. What is more, application of SNA may lead to (or be a tool of) stigmatization of particular groups, regarded as “suspect communities.” Furthermore, it may be one of the effects of criminalization through “being” instead of “doing.” Once again, such policing would be, without any exemptions, against the human rights system. As such, it highlights the necessity of avoidance of association of criminal activity with particular ethnicity, religion, or nationality.

If so, from the point of view of the human rights system, a legitimate application of SNA in reference to crime prevention and law enforcement is unavoidably connected with the necessity of fulfilment of various prerequisites. Some of them, as in the case of infringement of the right to privacy, are universal and possible to be listed. However, other requirements are related to particularities of the case itself. As such, at the abstract level it is only possible to indicate risks connected with them, instead of providing detailed lists of prompt solutions.

General conclusion that appears from presented deliberation is that effective crime prevention and law enforcement require use of various methods and techniques that derive from different fields of science. However, boundaries of application of such measures are provided by law, at either national or international level. One of such limitations is the human rights

system. As long as the use of particular method or technique fits into the requirements of the human rights and legal systems, and is useful to achieve the assumed legitimate purpose, its application should be allowable.

Last but not least, as it was mentioned, the main aim of this article was to present various risks and potential weak points connected with the use of SNA in crime prevention and law enforcement, related to particular aspects. However, I am fully aware that discussed issues are just a peak of an iceberg. What should be elaborated further are, for example, diverse aspects of making use of results of SNA during court trials, and other processes of judicial decision, detailed analysis of types of crimes that may be prevented with SNA, practical difficulties with application of this technique by the state organs. However, due to the complexity of these subject areas, they should be a matter of further research.

BIBLIOGRAPHY

PUBLICATIONS

1. Berlusconi G., *Do All the Pieces Matter? Assessing the Reliability of Law Enforcement Data Sources for the Network Analysis of Wire Taps*, "Global Crime" 2013, Vol. 14, Issue 1.
2. Berlusconi G., *Social Network Analysis and Crime Prevention*, [in:] *Crime Prevention in the 21st Century. Insightful Approaches for Crime Prevention Initiatives*, eds. B. LeClerc, E. Savona, Cham 2017.
3. Calderoni F., *The Structure of Drug Trafficking Mafias: the 'Ndrangheta and Cocaine*, "Crime, Law and Social Change" 2012, Vol. 58, Issue 3.
4. McCulloch J., Pickering S., *Pre-crime and Counter-terrorism. Imagining Future Crime in the 'War on Terror'*, "The British Journal of Criminology" 2009, Issue 49.
5. Papachristos A., Hureau D., Braga A., *The Corner and the Crew: The Influence of Geography and Social Networks on Gang Violence*, "American Sociological Review" 2013, Vol. 78, Issue 3.
6. Papachristos A., Wildeman Ch., Roberto E., *Tragic, But Not Random: The Social Contagion of Nonfatal Gunshot Injuries*, "Social Science & Medicine" 2015, Vol. 125.
7. Sentas V., *Policing The Diaspora: Kurdish Londoners, Mi5 And The Proscription Of Terrorist Organizations In The United Kingdom*, "The British Journal of Criminology" 2016, Vol. 56.
8. Scott J., *What is Social Network Analysis?*, London–New York 2010.
9. Yang Ch., Tang X., *Information Integration for Terrorist or Criminal Social Networks*, [in:] *Security Informatics. Outlines the Foundations and Parameters of the Field of Intelligence and Security Informatics (ISIS)*, eds. C. Yang, M. Chau, J.-H. Wang, H. Chen, Springer 2010.
10. Zedner L., *The Pursuit of Security*, [in:] *Crime, Risk and Insecurity: Law and Order in Everyday Life and Political Discourse*, eds. T. Hope, R. Sparks, New York 2000.

LEGAL ACTS

1. Communication Number 488/1992 of Human Rights Committee, *Toonen v. Australia*, [online] <http://hrlibrary.umn.edu/undocs/html/vws488.htm> [accessed: 1.04.2017].
2. Human Rights Committee, General Comment 16, 23 session, 1988, [online] <http://hrlibrary.umn.edu/gencomm/hrcom16.htm> [accessed: 1.04.2017].
3. *The right to privacy in the digital age*, Report of the Office of the United Nations High Commissioner for Human Rights, 30th of June 2014.
4. *The United Nations Global Counter-Terrorism Strategy Review*, Resolution of the General Assembly of UN number 70/91, [online] http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/70/291 [accessed: 1.04.2017].
5. *United Nations Declaration on Crime and Public Security*, Resolution of General Assembly number A/51/610, [online] <http://www.un.org/documents/ga/res/51/ares51-60.htm> [accessed: 1.04.2017].
6. *Universal Declaration of Human Rights*, Resolution of General Assembly number 217 A, [online] <http://www.un.org/en/universal-declaration-human-rights/index.html> [accessed: 1.04.2017].