*Marko MILOSAVLJEVIĆ, Jernej AMON PRODNIK and Lenart J. KUČIĆ**

SECURING THE COMMUNICATION OF JOURNALISTS WITH THEIR SOURCES AS A FORM OF SOURCE PROTECTION – EDITORIAL POLICY OF SLOVENIAN MEDIA REGARDING COMMUNICATION AND TECHNOLOGY

Abstract. *The rapid development and penetration of new communication and digital technologies is also affecting the transformations of journalistic procedures and practices within news production and the distribution and gathering of information. Journalistic communication and the protection of journalistic sources as one of the key mechanisms for establishing the news net and network of sources and for performing the function of reporting and fulfilling the role of 'watchdogs' is under threat. Analysis of in-depth, semi-structured interviews with editors of key Slovenian media shows a lack of systematic protection of journalistic communication and a lack of editorial policy regarding communication with journalistic sources. Certain individual considerations and measures are taken, although systematic editorial policy is still missing along with education regarding safe communication.*

Keywords: *journalistic sources, surveillance, editorial policy, the protection of communication, the protection of sources*

Introduction

The rapid development and penetration of new communication and digital technologies is also affecting the transformations of journalistic procedures and practices within news production and distribution as well as within the gathering of information. In this era of 'the Internet of things' where digital technologies penetrate everyday activities and life including

* *Marko Milosavljević, PhD, associate professor, Faculty of Social Sciences, University of Ljubljana; Jernej Amon Prodnik, PhD, postdoctoral researcher, Institute of Communication Studies and Journalism (PolCoRe Research Group), Faculty of Social Sciences, Charles University in Prague; researcher Social Communication Research Centre, Faculty of Social Sciences, University of Ljubljana; Lenart J. Kučić, MA, Delo publishing company, Ljubljana.*

areas in which digital technology and telecommunication were not present in the past, new ways and processes of news work, gathering information and communicating with sources are developing. At the same time, this enhanced power of communication technologies enables new opportunities for new forms of surveillance and abuses. Within this process, journalistic communication and the protection of journalistic sources as one of the key mechanisms for establishing the news net and network of sources and for performing the function of reporting and fulfilling the role of 'watchdogs' is under threat.

In the framework of wider developments in society related to the new technologies, we are witnessing changing conceptualisations of citizenship and social life in the digital age, with privacy and security establishing themselves as foundational issues of existing societies (Rainie and Anderson, 2014). Global political, economic and social lives are increasingly reliant on technological platforms and ICT, which are not only vulnerable to, but may even facilitate, mass surveillance (Mattelart, 2010; General Assembly, 2014; Greenwald, 2014). As the infamous whistle-blower Julian Assange (2014) noted, "the very concept of the Internet – a single, global, homogenous network that enmeshes the world – is the essence of a surveillance state" (cf. Mathiesen, 2013: 19). Hill (2012: 109) similarly noted how "the increasing computerization of all aspects of society is directly linked to new potentials for all-encompassing surveillance".

In a parallel process, media industries and with them journalistic practice have in recent years undergone significant transformations: technological changes and the relatively unsuccessful adaptation of old media to digitalisation (Milosavljević and Kerševan Smokvina, 2013); economic crisis both globally and locally (Vobič et al. 2014); collapsing economic models of traditional mass media industries, which have led some authors to claim that we may very well be witnessing 'the death of journalism' as we have so far known it (McChesney and Nichols, 2012). These are only some of the perturbations the media and journalism are facing today.

Most of these transformations in media industries have been relatively well documented in both a general sense and with a detailed analysis of specific cases. But they have rarely (if at all) been connected to another overwhelming and significant social trend that was mentioned above, namely, the rise of what different authors have come to call 'the surveillance society' (see Lyon, 1994). The expansion and intensification of surveillance practices have at least indirectly, if not directly, influenced most facets of social life. Some authors even claim that we are witness to the emergence of liquid surveillance, which is spreading and permeating throughout most social spheres and areas of our lives, even those that have never before been put under such scrutiny (Lyon and Bauman, 2013). Surveillance has an

increasingly important role in journalism and journalistic practice, but these issues have only occasionally been seen as important elements of the work of journalists, while systematic analyses of the influence of surveillance on journalistic practice have been even more sporadic. There is thus an important research gap regarding the protection of journalistic sources and practice of journalists in the context of the new surveillance technologies.

To fill this research gap, the article analyses the connection between the expanding surveillance apparatus and new forms of tracking people with how journalists and editors respond to these changes in their daily journalistic practices and in which ways this impacts on their work. We particularly focus on the issue of protecting journalistic sources and their anonymity. Our aim in the research was to answer the following research questions:

RQ1: How is the Slovenian media protecting the privacy of their journalists' communication?

RQ2: What kind of editorial policies or rules of communication (if any) have been established that are followed by journalists when dealing with confidential sources that would help protect their identities when communicating digitally?

Based on in-depth, semi-structured interviews, our qualitative empirical research therefore focused on how journalists and editors have adapted to the intensification of surveillance and its extension throughout different social spheres. We were interested in whether journalists and editors have changed their day-to-day activities and practices, including the techniques used to protect their sources, or whether they feel that this does not concern their work. We also wanted to answer to what extent these actors are aware of the dimensions of electronic surveillance taking place today. These queries can aid in probing a more general problem, namely, how is the role of journalism changing in an era of ubiquitous mass surveillance. The article first focuses on the development of global surveillance in relation to digital ICT and different social antagonisms (part 2), before connecting these pertinent issues to journalism (part 3) and then to the specific empirical case of the daily practices of Slovenian journalists and editors (parts 4 and 5).

The Global Surveillance Society and Digital Information and Communication Technologies

Information systems are part and parcel of human societies, with communication and the exchange of information often considered a prerequisite for social and political relations (Headrick, 2000). Yet information systems are also intrinsically connected to monitoring (Mathiesen, 2013: 23–25). In Mathiesen's (2013: 23) view, information and surveillance systems "have probably existed in some form in States in all ages". Even though the

(ab)use of information systems for the purpose of monitoring has existed since the development of complex human societies, these practices fundamentally changed with the rise of modernity and capitalist social relations. Surveillance became systematic and broad-scale, a means of both social control and power (Lyon, 1994: 24). At the start of the 1990s, Lyon (1994) coined the concept of the "surveillance society" and noted how to an "unprecedented extent, ordinary people now find themselves 'under surveillance' in the routines of everyday life" (ibid.: 4).

Lyon's (1994) account is one of the earlier warnings about the pervasiveness of modern surveillance. But recent social antagonisms coupled with developments in ICT have brought about an even more significant upsurge in the monitoring of persons, groups and even entire populations. Different authors carrying out research in this area emphasise that we are witnessing the persistent intensification of surveillance as well as more extensive and all-encompassing forms of surveillance (see, for example, Lyon, 2002; Ball and Webster, 2003; Mattelart, 2010; Andrejevic, 2007; 2012; Fuchs et al. 2012; Allmer, 2012; 2014; Mathiesen, 2013; Mosco, 2014: 137–155; Greenwald, 2014). In fact, according to Lyon (2002) surveillance has now become one of the most fundamental aspects of modern societies. It continuously flows through different social spheres, successfully adjusting to the specifics of every one of them. The final result, in Mattelart's (2010: 198) view, is that "a new mode of governing society by tracking is now emerging, in which everyone who circulates is liable to be under surveillance".

Digital Information and Communication Technologies and Ubiquitous Surveillance

The increased capacities and possibilities for surveillance can be associated with technological advances. New ICT provides fresh options for gathering, collecting, storing and analysing data. This has made it much simpler to monitor what was previously an almost unimaginable plethora of social relations. The new surveillance technologies enable extensive and intensive large-scale surveillance with great precision (see Allmer, 2012: 99). With the assistance of digital technologies, surveillance is therefore encompassing more social activities more efficiently, while requiring less human input. It is regularly performed in an indirect and invisible manner, with people often voluntarily tolerating it (Andrejevic, 2007; Allmer, 2012; Lyon and Bauman, 2014).

Digital ICT is permeated with contradictions which in many ways reflects the contradictory nature of the capitalist societies in which they developed (see Andrejevic, 2009; Fuchs, 2009; Amon Prodnik, 2014). They have been hailed as the harbingers of democratic empowerment and user participation,

celebrated as sources of decentralised and subversive political action, individual freedom and democratic participation (e.g. Benkler, 2006). They have simultaneously also paved the way for new forms of enclosures, surveillance and exploitation. As emphasised by Andrejevic (2012: 82), interactive technologies "facilitate new forms of collaboration and communication as well as the enhanced ability to access and share information rapidly at a distance", but they also "represent the next stage of the colonization of social life by commerce and marketing" and facilitate other forms of social control.

Critical scholars analyse surveillance particularly in the light of the existing asymmetries and inequalities in social relations, which are fundamentally connected to the unequal distribution of different forms of power in capitalist societies (see Andrejevic, 2007; 2009; Mattelart, 2010; Fuchs et al., 2012; Hill, 2012; Allmer, 2012; 2014; Amon Prodnik, 2014). Inequalities extend to digital environments and it is exactly *mass* surveillance that demonstrates them in their entirety. Only powerful actors can store and analyse the big data gathered through monitoring and tracking of vast numbers of people, which means that mass surveillance can be seen as a form of domination because it is largely restricted to the social elite (ibid.).

The Globalisation of Ubiquitous Surveillance after 9/11

Even though digital ICT and surveillance are not a novelty, the major turning point in global surveillance was not technological *per se*. Surveillance capacity is not an inherent quality of digital ICT, but something that is embedded in it and (ab)used because of political, economic and social pressures, influences and antagonisms. Even though digitalisation coincides with increasingly invasive and detailed surveillance – and can even be seen as a precondition of it – these processes did not occur because of technology. First, they ought to be attributed to the Cold War antagonisms and to the close historical interconnections between military apparatuses and communications, including the planned development of surveillance systems (Mattelart, 2010; Schiller, 2011; Amon Prodnik, 2014). Second, they must be related to a major social event, namely the September 11 attacks, and the consequent launching of the War on Terror doctrine.

After 9/11 a plethora of measures, regulations and advanced surveillance systems were implemented, leading to similar developments both across Europe (Mathiesen, 2013) and globally (Mattelart, 2010), with the United States of America leading the way in the expansion and intensification of mass global surveillance (ibid.: 141–147; Ball and Webster, 2003; Schiller, 2011: 278). The 9/11 attacks and surrounding moral panic led to public calls for greater surveillance by all means necessary. This context provided fertile ground for the legitimisation of indiscriminate mass surveillance and

for political authorities to change legislation accordingly (ibid.; also see Maxwell, 2003; Mattelart, 2010; Schiller, 2011).

However, it was only with the disclosures of the whistle-blower Edward Snowden, connected especially to the activities of the American National Security Agency (NSA), when the extent of the global surveillance apparatus was revealed in its entirety. As he emphasised, the NSA was "building a system whose goal was the elimination of all privacy, globally. To make it so that no one could communicate electronically without the NSA being able to collect, store, and analyze communication" (Snowden in Greenwald, 2014: 47–48). The vastness of the NSA's surveillance system and its 'collect it all' aspirations become obvious when we bear in mind that its interception system is capable of reaching three-quarters of *all* Internet traffic in the USA (ibid.: 98–99). While the scale of surveillance has surprised even the pessimists, perhaps the most troubling is the fact that the surveillance happened with little accountability, transparency or clear-cut limits in place to create certain checks and balances in the system (Greenwald, 2014: 90).

Journalism and Surveillance

The trend of expanding government surveillance is worrisome as it has been documented to have an impact on freedom of expression. As Greenslade (2014) points out, the treatment of journalists as criminals or using their private phone conversations as ways of investigating crime leads to scaring off whistle-blowers and in effect negatively influences the public's right to know. Guy Berger, director of UNESCO's Division of Freedom of Expression and Media Development, is similarly convinced that whistleblowers will fear contacting journalists if they have reason to doubt the related confidentiality, which potentially may lead to less news about corruption or abuse in the public domain (Posetti, 2014b: 38). Further, there is evidence of an emerging trend of journalistic self-censorship. In the United States a survey of over 520 American writers about the effects of surveillance on their work has shown that up to 16 percent of respondents claimed to have refrained from conducting Internet searches or visiting websites on topics that may be considered controversial or suspicious, while another 12 percent have seriously considered refraining from it (PEN American Center, 2013). Such trends are now evident even on a global scale: in 2015, the concern about surveillance was nearly as high among writers living in democracies (75 percent) as among those living in non-democracies (80 percent), while an increasing trend of self-censorship has also been reported by writers living in democratic countries (ibid.).

Global Trends Connected to the Surveillance of Journalists

As privacy is compromised in the era of digital surveillance – which inevitably leads to threats regarding the anonymity of journalistic sources – a clear need to protect both their sources and themselves has emerged (IJNet, 2014). As acknowledged by UNESCO (2013), "privacy is essential to protect journalistic sources, which enable a society to benefit from investigative journalism, to strengthen good governance and the rule of law/.../". The omnipresent electronic surveillance and its invasion of privacy raises the important issue of whether journalists can still promise anonymity to their sources.

Communication technologies have made surveillance, interception and data collection easier. They have eradicated financial or practical disincentives to conducting surveillance and made the state's effectiveness in conducting surveillance no longer limited by scale or duration (General Assembly, 2014). In the last couple of years this has paved the way for the emergence of a trend that compromises the principle of the confidentiality of journalists' sources: national security agencies in various parts of the world have gained access to journalists' data, such as documents, emails and phone records, thus making journalists, sources and whistle-blowers vulnerable to tracking (UNESCO, 2014: 30). This has been especially evident in the revelations of Edward Snowden. It was, for example, disclosed that the Government Communications Headquarters (GCHQ), the British intelligence and security organisation, which regularly cooperated with NSA, has saved emails to and from journalists (cf. Greenwald, 2014). Emails from some of the US and the UK's largest media organisations, including the BBC, Reuters, the Guardian, the New York Times, Le Monde, the Sun, NBC and the Washington Post, were saved by GCHQ and shared on the agency's intranet as part of a test exercise by the signals intelligence agency (Ball, 2015).

The Protection of Sources in an Era of Surveillance

In these circumstances, one of the defining questions is whether journalists can still promise anonymity to their sources. There is simultaneously an indisputable need to adjust journalistic practices to the altered conditions of their work. As pointed out by Bell (2014), "the tools we use for journalism – Gmail, Skype, social media – are already fatally compromised by being part of a surveillance state".

Practices in investigative reporting and source protection therefore need to change, but their evolution has not been easy (Coll, 2014). Numerous tools are available that enable anonymous navigation online, telephone encryption and tools to encrypt instant messaging (IJNet, 2014) or apps

like Facebook's WhatsApp and Apple's iPhone, as the companies say they do not have the means to unlock them even when they receive valid law-enforcement requests (Gauthier-Villars and Schechner, 2015). But a reporter's communication is quite extensive and its encryption takes both time and effort (Coll, 2014). In addition, reporters do not always have the technical skills to ensure their practices are effective and efficient (ibid.). However, as noted by Posetti (2014a: 33), surveillance is bound to change the behaviour of journalists and journalistic practice; the industry is bound to completely rethink how to deal with their sources, with people and with whistle-blowers who provide them with information.

Research Overview and Methodology

There is a research gap in scholarly literature when it comes to a systematic analysis of how the intensification and extension of surveillance influences day-to-day journalistic practice. Our empirical research thus focused on how journalists and editors in Slovenia have adapted to the social context in which surveillance has become omnipresent, and to what extent they are aware of the magnitude of the electronic surveillance taking place in different social spheres. Our intention was to answer the following research questions: How is the Slovenian media protecting the privacy of their journalists' communication? What kind of editorial policies or rules of communication (if any) have been established that are followed by journalists when dealing with confidential sources to help protect their identities while communicating digitally? By answering these queries, we can also more generally ascertain in which ways the role of journalism is changing in this era of ubiquitous mass surveillance.

It is first worth noting, as part of our research, that the assessed Slovenian media institutions have no written policies or guidelines on how their employees should use electronic communications (e.g. their electronic mail, mobile phones or web applications). A reasonable way of gaining an insight into the journalistic practices and editorial processes in the newsrooms was thus by conducting in-depth qualitative interviews with editors and senior journalists. The method of semi-structured, face-to-face interviews (see Deacon et al., 1999: Ch. 4), which is a commonly accepted method in the academic community and one of the most important qualitative methods (ibid.; Flick, 2007; Kvale, 2007), was consequently adopted for our empirical analysis. Such interviews enable a better insight into editorial and journalistic processes compared to "abstract descriptions or attempts with formalised procedures" (Morrison and Tumber, 1988: X). Interviews are particularly appropriate for analysing and understanding individual perspectives of different actors (Lindlof, 1995; Chung, 2007). This is especially viable for

a semi-structured interview with its main advantage, namely that it offers an insight into the world of opinions of the interviewees (Bryman, 2008: 438).

Twelve Slovenian media institutions were included in the study, with both traditional (newspapers, magazines, television) and online media being represented. The institutions selected for the analysis reach a vast majority of media audiences in Slovenia, while producing nearly all relevant journalistic content in this country and providing comprehensive coverage of all important political, economic and social issues. The approached interviewees come from companies that represent diverse ownership structures (domestic and foreign ownership, strategic or non-strategic owners), business models (commercial and public television, paid newspapers, commercial online sites, and a non-profit online portal), editorial orientations (political magazines, investigative and general interest journalism), and media platforms (traditional, online only, integrated). Differences between the various institutional backgrounds of the interviewees contribute to a sufficiently heterogeneous sample of the interviewees and result in sufficiently diverse newsroom cultures and journalist practices to offer a representative overview of Slovenian journalism, while quite possibly also reaching a point of knowledge saturation (on qualitative sampling, see Flick, 2007: Ch. 3; cf. Kvale, 2007: 43–45).

Altogether, 13 journalists and editors were interviewed for the study. Five respondents were female and eight male. Eight of the interviews were carried out by Lenart J. Kučić, himself a practising journalist at Delo, a leading Slovenian national newspaper, and five by Marko Milosavljević, associate professor at the Department of Journalism, Faculty of Social Sciences, Ljubljana. The interview sample includes: the editor-in-chief of the national press agency; the editor-in-chief of the biggest commercial television; the deputy of the editor-in-chief of the biggest national daily; a business correspondent and investigative journalist (representing the editor-in-chief of the second biggest national daily); the editor-in-chief of a national business daily; the editors-in-chief of two different political weekly magazines; the editor-in-chief of the biggest non-legacy online portal (news and general interest); the editors of two different political, weekly television current affairs shows; the editor-in-chief and founder of an Internet media start-up specialising in investigative journalism; and a senior investigative journalist of the third biggest national daily (on behalf of the editor of that daily). The interviews were conducted either in the editorial offices of the respondents or in public places (for example in cafes and pubs) between February and April 2015. The interviews lasted 45 to 90 minutes; they were recorded, transcribed and analysed. At the time of the interviews, all of the respondents had senior editorial or executive roles in their institutions, except for the two respondents who were put forward for the interview by their editors

as being more competent in the field of the conducted research. Our aim in selecting people with senior roles in media institutions was to construct a sample of interviewees who on one hand were supposed to have an overview of these issues in their organisations while, on the other, they should also (at least formally) carry a large degree of responsibility.

Even though the conducted interviews were semi-structured in delivery, they remained standardised through the following questions which were put to all of the respondents: How well are you aware of the extent of global/local electronic surveillance? Are software and hardware tools used to ensure safer electronic communications (e.g. crypto phones, virtual private networks, PGP encryption for email, secure messaging apps, encrypted voice apps)? Which safety procedures are followed when protected sources are contacted or when there is a need to exchange sensitive information? Has your institution adopted (or intends to adopt) a more secure communications strategy to better protect journalists and their sources from electronic surveillance? In line with these questions, it can be stated that a type of 'factual interview' was conducted. According to Kvale (2007: 70), such interviews "are in accord with a miner metaphor of interviewing, in seeking facts and concepts that are there already". The focus was less on the interviewee's own perspective or subjective meanings and more on acquiring valid information about *the state of things* in the practices of the newsrooms (ibid.: 71).

Results of the Research

The Lack of Security Policies as a General Trend

The interviews demonstrated that no media institution has adopted a security policy or implemented any specific measures to improve the protection of their journalists and their sources from electronic surveillance. At the time of the interviews, there was also no intention to adopt such policies in the near future, even though all of the respondents said they are 'well aware' of the possibilities and potential misuses of electronic surveillance in their journalistic work.

All interviewees agreed that the new forms of surveillance are a problem for journalists and media institutions, which are generally not well prepared for the digital age. However, only one respondent pointed out actual use of software tools for encrypting communications: the founder and editor of an online media start-up specialising in investigative journalism. This interviewee used security apps for encrypting text messages and phone calls on his smartphone and locked his computer with strong encryption (computer drives, USB keys).

The general trend, which points to the lack of serious security policies adopted by media institutions, is best demonstrated by a senior investigative journalist who noted that they have "got absolutely no training in how and when to use security apps or encrypt our communication. This area is left to each journalist to deal with it as he or she knows". He also pointed out "this topic was never even discussed". This issue was not on the agenda even when the journalists asked the editors to organise training in security.

"Our news staff has warned us that they would like to have a seminar on safe communication. However, we have not developed any exact protocols regarding the communication with our sources so far, or in communication among ourselves", explained the senior editor of one media company. "At the moment, we have a newsroom that is non-stop open. We do not even have a doorman or security guy at the entrance to our premises. In the evening, I guess it is very easy to enter our newsroom and offices and install eavesdropping equipment".

The only exception to this rule was the online media start-up because its staff needed to follow security recommendations in order to cooperate and exchange information with other investigative journalistic centres in the region (they used security software and organised training for their journalists). "Also, we hope to earn the trust of potential whistle-blowers. Nowadays, the people with access to information are often geeks – computer programmers and techies – who will not use unsecure communication channels when they decide to contact you. The use of security tools is a must for such sources", the editor and founder of the investigative portal emphasised.

Returning to 'Analogue' Communication

How do Slovenian media institutions therefore protect their sources and journalists from electronic surveillance when no standardised policies have been adopted? The usual procedure was best described by the editor of a television weekly magazine on a commercial television channel: "I prefer James Bond to Edward Snowden. When it becomes sensitive, I turn from digital to analogue", she pointed out. According to her, "returning to analogue" means no phone conversations, no text messages and no emails. Her journalists exchange information on USB memory keys or printed on paper. They meet their sources in person, find a hidden or busy public location, with a lot of background noise, and leave their mobile phones at home or in the office.

Most respondents gave similar replies and explained that opting for analogue communication is not a new strategy. "My first editor taught me not to use a phone when I am having a sensitive conversation. That was 20

years ago, before Snowden and email", said the editor of a television weekly magazine on a commercial television channel. "Decades ago, we were using phone booths, now we use unregistered mobile phones and anonymous emails", said the editor of a political weekly. "Another useful trick was to use couriers and middlemen to protect the source. We still do that", he added.

The editor of a business daily said they are also using middlemen to protect sources. Further, they remove any metadata from documents before publishing them (e.g. watermarks, file information...). They do not keep any digital or physical copies of sensitive documents on computers or in their offices. Instead, they entrust them with their legal representative. In addition, only an insider can provide an important document and he knows the risks. According to the business editor, this means such a person can protect himself much better than any journalist could protect him or her.

Two respondents also mentioned some non-analogue methods of more secure communications: the use of web services for voice calls (e.g. Viber) instead of phone calls, setting up anonymous email accounts to communicate with sources, and using public online access (e.g. a cybercafé or a public hotspot) instead of an institution's own access or a home network.

Fear of Paranoia

Only one respondent – the editor of the second biggest political weekly – held a different view to those presented above. He strongly argued against the need for secure communications and claimed that adopting security measures would mean "accepting the dictatorship of fear and paranoia. Journalists are not spies or secret police and they should not behave like them. They should operate within the legal framework and their privacy should be protected by law, not by some kind of apps".

Both editors of the television magazines shared some of his beliefs. "I realise that electronic surveillance has become cheap. Many organisations and even individuals can afford specialised gear to break into computers and intercept mobile phone calls. I am not concerned about police or the secret service. What worries me are former spies, criminals, and detective agencies that provide information to political parties and lobbies", said the first editor, who then continued: "But I do not want to become paranoid. I say to myself: I am not doing anything illegal. I am a journalist and it is my right to communicate freely. I do not want to be paralysed by a fear of who is listening to my conversation and how they will use this information against me".

The editor of a television magazine on a public television channel offered a very similar explanation (and so did the business correspondent of the second biggest national daily), while also admitting that she does not

have technological competence to protect herself from electronic surveillance: "I believe that most Slovenian journalists do not have enough skills to stay secure online".

No Sources, No Secrets

The lack of proper skills to protect themselves and a fear of unreasonable paranoia are not the only reasons that Slovenian editors do not use or encourage the adoption of software and hardware tools to ensure safer electronic communication. As noted by the founder and editor of the online media start-up: "Slovenia is not like the USA. If you want to meet a source, you often just take a walk. You do not need to fly to the other coast to have a meeting". It may make no financial or even practical sense to invest a lot of money to create or adopt a secure solution for electronic communication (and something similar can be said for building an Internet platform for publishing sensitive leaks, which would be comparable to that of WikiLeaks), when whistle-blowers can use much simpler solutions, for example sending an envelope to a journalist or giving documents to a middleman.

The editor of the business daily had a different explanation: "We do not have a Slovenian version of Edward Snowden or Julian Assange. There are only two or three potentially important leaks we get every year. Most Slovenian journalists have never handled any sensitive information and I can hardly imagine them as targets of electronic surveillance". The editor of the business daily was not the only respondent who doubted the investigative skills of Slovenian journalists. Even the editors and journalists themselves believed they have nothing to hide and they are not covering anything sensitive. The editor of the online news portal admitted that none of his journalists "could do investigative journalism".

The founder and editor of the online journalism start-up was even more direct in his critical appraisal of the (non)existence of investigative practices: "Do you know what investigative journalism means in Slovenia? You get an anonymous document from someone and publish it without checking the facts or verifying the sources. You do not invest weeks or even months in your own research. So why would you protect your information and your sources if you do not have any?". He also noted that journalist practices will not change as long as journalists and editors rely on their traditional sources, namely politicians, public officials and lobbyists. "We need a Snowden moment to change – when an important whistle-blower will only communicate with a skilled journalist who can use PGP keys and other crypto-tools".

Journalists under Surveillance?

The editor of a television current affairs programme at the public broadcaster speculated that only a scandal could change the behaviour of Slovenian press rooms: "Media institutions would probably react if we got solid proof that journalists are under surveillance. We often hear rumours and speculations about illegal electronic eavesdropping but we do not take them very seriously", he stressed.

This editor of a television current affairs programme was not the only one to mention rumours and speculations about illegal electronic eavesdropping. "I have no illusions that we are not subjected to such eavesdropping now and then", the editor of the Slovenian press agency admitted. A senior investigative reporter at a national daily was even more explicit: "I have realised twice that someone went through my official e-mail, but our IT people could not explain who it was. A number of times I have also noticed that someone from a distant computer had opened my folders. I have set the folders according to the dates of last changes and, every now and then, suddenly a folder pops on top that I have not opened in a long time".

"Telephone communication is a special story: it often happens that during sensitive calls a line breaks or you cannot understand a word due to an interrupted signal. Once it even happened that there was beeping and screeching because of microphone interference". Furthermore, the respondent not only expressed distrust in anonymous eavesdroppers: "There are also serious signals that our official email folders are being supervised upon the order of our owners or editors by our own IT personnel", he claimed.

Conclusion

The development of new digital communication platforms and surveillance techniques has brought new possibilities for mass surveillance and targeted surveillance. This includes journalists, editors and their communication with their confidential sources. The watchdog function of the media is also enabled by the strict confidentiality of sources when practising investigative reporting, although new technologies are putting this confidentiality under increasing threat. The issue of new communication practices and procedures by journalists when gathering information within the context of the new, ubiquitous surveillance has, however, not been researched adequately and therefore an important research gap was left within the research of contemporary journalism and media practices. This paper analysed the awareness of journalists and editors of the issue of protecting the confidentiality of sources in the era of 'the Internet of things' and new surveillance techniques, as well as the development of new practices of news gathering

as a consequence of this new environment. The responsiveness of editors and journalists of key media outlets in Slovenia as an example of a smaller country with a particular setting for journalistic sources, communication, and the protection of identity, as well as specific journalistic practices and education, was analysed for the first time in the context of the new digital environment.

The research shows a strong contradiction between the reported awareness and actual behaviour of Slovenian journalists and editors. All but one interviewee agreed that the new forms of surveillance are a problem for journalists and pose a real threat to their profession. They were concerned about the possibilities and potential misuses of electronic surveillance to control their work, trace journalists' sources, and prosecute whistle-blowers. One-third of the interviewees mentioned the possibility that state agencies or private companies are already gathering information from journalists and listening to their conversations when they cover sensitive stories. One interviewee explicitly described suspicious "clicks and pops" in his phone and reported "the strange behaviour" of his office computer.

On the other hand, only one respondent pointed out actual use of software tools for encrypting communications. The interviews that were conducted demonstrate that no media institution has adopted a security policy or implemented any specific measures to improve the protection of their journalists and their sources from electronic surveillance. At the time of the interviews, there was no intention to adopt such policies in the near future – despite the fact that the journalists themselves had suggested they needed security training. Some training and workshops have been organised by NGOs and the Slovenian Association of Journalists in the last two years but only one interviewee had attended such a workshop. The interviews showed that a number of journalists are aware of the issues related to potential surveillance and new technologies; however, the lack of a formal response and guidelines of their media establishments shows slow responsiveness and awareness on the official, institutional level, leaving individual journalists to their own considerations and decisions.

Most interviewees believe that traditional ('analogue') security strategies are also suitable for the digital age (meeting in person, use of middlemen etc.). However, they fail to recognise the surveillance possibilities of big data analysis, the collection of metadata, and cloud computing that cannot be avoided by simply turning off the phone when meeting a source.

The results therefore show several important characteristics of the analysed media and interviews with the journalists and editors. The lack of any adoption of security policies can be seen as a general trend within the analysed media. Opting for 'analogue' communication is seen as the key and most frequent response by those aware of the issues raised by new digital

platforms. This is complemented by a lack of proper skills to protect themselves and a fear of unreasonable paranoia, as well as the issue of the lack of a specific case that would increase journalists' awareness of the possibility and extent of surveillance within the specific (Slovenian) society.

However, the study also reveals strong scepticism among editors and journalists that Slovenian newsrooms actually engage in investigative reporting. The low level of awareness or practice of protecting the communication and confidentiality of sources is also a consequence of the general practice of journalism within a small society and economic pressures, namely the practice of collecting information mainly through routine sources such as press releases and pseudo-events (like press conferences). There is a significant lack of investigative journalism practices and procedures, reflected in the small number of stories that rely on confidential sources. Hence, journalists often do not need to protect any information or a source. This result is perhaps the most significant and worrisome as it shows that journalistic production in Slovenia predominantly relies on public relations services and sources. This result also points to an important failure to fulfil the role of watchdogs as one of the key aspects and roles of journalism and the media in a democratic society. On the other hands it opens the issue of the strategic position of journalists and media in today's society: the watchdogs are being watched and controlled by those who they themselves were supposed to watch and control. The roles are being reversed within the new communication and power asymmetry.

The study is based on in-depth interviews and journalistic perceptions. We are aware that the use of different methods could lead to additional understanding of journalistic practices in the context of new surveillance issues, particularly with the use of ethnographic methods (Schultz, 2007), or through content analysis or the relationships in communication processes (Livingstone, 2003). These approaches could provide another perspective on news gathering processes and the protection of journalistic sources, and therefore represent an area of possible further research. A further insight would be provided by a wider pattern of interviewees – we are aware of the 'small-n problem' (see, for example, Lieberson, 1991) – and additional journalists, but also journalistic sources could offer a more complex perspective on the issue of the protection of communication with sources. An international context of the study that would provide a comparative perspective by including journalists and editors in different countries could also represent a relevant addition to and wider setting for the issue. The issue of new surveillance techniques and their effects and consequences for journalistic practices and the protection of sources is an important topic for digital-era journalism and societies that affects the practices and role of journalism in political and societal processes. It will need to be regularly addressed in

various societies through different technologies and practices in order to appropriately assess these transformations.

BIBLIOGRAPHY

Allmer, Thomas (2012): Towards a Critical Theory of Surveillance in Informational Capitalism. Frankfurt, Berlin, New York, Oxford: Peter Lang.

Allmer, Thomas (2014): (Dis)Like Facebook? Dialectical and Critical Perspectives on Social Media. Javnost – The Public 21 (2): 39–56.

Amon Prodnik, Jernej (2014): The Brave New Social Media: Contradictory Information and Communication Technologies and the State-Capitalist Surveillance Complex. Teorija in Praksa 51 (6): 1222–1241.

Andrejevic, Mark (2007): iSpy: Surveillance and Power in the Interactive Era. Kansas: University Press of Kansas.

Andrejevic, Mark (2009): Critical Media Studies 2.0. Interactions: Studies in Communication and Culture 1 (1): 35–51.

Andrejevic, Mark (2012): Exploitation in the Data Mine. In Christian Fuchs et al. (eds.), Internet and Surveillance: The Challenges of Web 2.0 and Social Media, 71–88. New York, London: Routledge.

Ball, Kirstie and Frank Webster (eds.) (2003): The Intensification of Surveillance. London: Pluto Press.

Benkler, Yochai (2006): The Wealth of Networks: How Social Production Transforms Markets and Freedom. New Haven, London: Yale University Press.

Chung, Deborah Soun (2007): Profit and Perils: Online News Producers' Perceptions of Interactivity and Uses of Interactive Features. Convergence: The International Journal of Research into New Media Technologies 13 (1): 43–61.

Deacon, David, Michael Pickering, Peter Golding, and Graham Murdock (1999): Researching Communications: A Practical Guide to Methods in Media and Cultural Analysis. London, Sydney, Auckland: Arnold.

Flick, Uwe (2007): Designing Qualitative Research. Los Angeles, London, New Delhi: Sage.

Fuchs, Christian (2009): A Contribution to Theoretical Foundations of Critical Media and Communication Studies. Javnost – The Public 16 (2): 5–24.

Fuchs, Christian, Kees Boersma, Anders Albrechtslund and Marisol Sandoval (eds.) (2012): Internet and Surveillance: The Challenges of Web 2.0 and Social Media. New York, London: Routledge.

Greenwald, Glen (2014): No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State. New York: Metropolitan Books.

Hill, David W. (2012): Jean-François Lyotard and the Inhumanity of Internet Surveillance. In Internet and Surveillance: The Challenges of Web 2.0 and Social Media, eds. Christian Fuchs, Kees Boersma, Anders Albrechtslund and Marisol Sandoval, 106–123. New York, London: Routledge.

Kvale, Steinar (2007): Doing Interviews. Los Angeles, London, New Delhi: Sage.

Lieberson, Stanley (1991): Small Ns and Big Conclusions: An Examination of the Reasoning in Comparative Studies Based on a Small Number of Cases. Social Forces 70 (2): 307–320.

Lindlof, T. R. (1995): Qualitative Communication Research Methods. Thousand Oaks: Sage

Livingstone, Steven, W. Lance Bennett and Howard Tumbler (2003): Gatekeeping, Indexing, and Live-event News: Is Technology Altering the Construction of the News? Journalism: Critical Concepts in Media and Cultural Studies 20 (4): 363–380.

Lyon, David (1994): The Electronic Eye: The Rise of Surveillance Society. Minneapolis: University of Minnesota Press.

Lyon, David (2002): Surveillance Studies: Understanding visibility, mobility and the phonetic fix. Surveillance & Society 1 (1): 1–7.

Lyon, David and Zygmunt Bauman (2013): Liquid Surveillance: A Conversation. Cambridge, Malden: Polity.

Mathiesen, Thomas (2013): Towards a Surveillant Society: The Rise of Surveillance Systems in Europe. Hook: Waterside Press.

Mattelart, Armand (2010): The Globalization of Surveillance. Cambridge, Malden: Polity Press.

Maxwell, Richard (2003): Herbert Schiller. Lanham: Rowman and Littlefield.

McChesney, Robert W. and John Nichols (2012): The Life and Death of American Journalism. New York: Nation Books.

Morrison, David E. and Howard Tumber (1988): Journalists at War: The Dynamics of News Reporting During the Falklands Conflict. London: Sage.

Mosco, Vincent (2014): To the Cloud: Big Data in a Turbulent World. Boulder: Paradigm.

Schiller, Dan (2011): The Militarization of US Communications. In Janet Wasko, Graham Murdock and Helena Sousa (eds.), The Handbook of Political Economy of Communications, 264–282. Malden, Oxford: Wiley-Blackwell.

Schultz, Ida (2007): The Journalistic Gut Feeling. Journalism Practice 1 (2): 190–207. Available at http://diggy.ruc.dk/bitstream/1800/6749/1/The_Journalistic_Gut_Feeling.pdf?origin=publication_detail, 10. 4. 2015.

Vobič, Igor, Sašo Slaček Brlek, Boris Mance and Jernej Amon Prodnik (2014): Changing Faces of Slovenia: Political, Socio-Economic and News Media Aspects of the Crisis. Javnost – The Public 21 (4): 77–98.

SOURCES

Assange, Julian (2014): Who Should Own the Internet? Available at http://www.nytimes.com/2014/12/04/opinion/julian-assange-on-living-in-a-surveillance-society.html, 12. 5. 2015.

Ball, James (2015): GCHQ captured emails of journalists from top international media. Available at http://www.theguardian.com/uk-news/2015/jan/19/gchq-intercepted-emails-journalists-ny-times-bbc-guardian-le-monde-reuters-nbc-washington-post, 27. 4. 2015.

Bell, Emily (2014): It's time to make up or break up – Emily Bell's seminal speech on the relationship between journalism and technology. Available at http://blog.wan-ifra.org/2014/11/26/emily-bells-semin al-speech-on-the-relationship-between-journalism-and-technology-its-time, 16. 5. 2015.

Benkler, Yochai (2013): The Dangerous Logic of the Bradley Manning Case. Available at http://www.newrepublic.com/article/112554, 27. 5. 2015.

Coll, Steve (2014): How Edward Snowden Changed Journalism. Available at http://www.newyorker.com/news/daily-comment/snowden-changed-journalism, 26. 5. 2015.

Gauthier-Villars, David and Sam Schechner (2015): Tech Companies Are Caught in the Middle of Terror Fight. Available at http://www.wsj.com/articles/tech-companies-are-caught-in-the-mi ddle-of-terror-fight-1424211060?mod=e2fb, 25. 5. 2015.

General Assembly (2014): The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights A/HRC/27/37. Available at http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf, 26. 5. 2015.

Greenslade, Roy (2014): Plebgate fallout: police appear to have declared war on journalists. Available at http://www.theguardian.com/media/2014/nov/30/plebgate-police-war-on-journalists, 13. 5. 2015.

IJNet (2014): 8 tools for greater digital security in 2015. Available at http://ijnet.org/en/blog/8-tools-greater-digital-security-2015, 25. 5. 2015.

Milosavljević, Marko and Tanja Kerševan Smokvina (2013): Mapping Digital Media – Slovenia. London: Open Society Foundation. Available at http://www.opensocietyfoundations.org/sites/default/files/mapping-digital-media-slovenia-20130605.pdf 12. 4. 2015.

Naim, Moises and Philip Bennett (2015): 21-century Censorship. Available at http://www.cjr.org/cover_story/21st_centur y_censorship.php?page=all, 20. 5. 2015.

PEN American Center (2013): Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censor. Available at www.pen.org/sites/default/files/Chilling%20Effects_PEN%20American.pdf, 19. 5. 2015.

Posetti, Julie (2014a): Shielding journalism in the age of surveillance. In Shaping in the Future of News Publishing – Trends in Newsroom 2014. Darmstadt: World Editors Forum.

Posetti, Julie (2014b): Shielding journalism in the age of surveillance. Interview: Global action on rights to privacy and freedom of expression: Guy Berger. In Shaping in the Future of News Publishing – Trends in Newsroom 2014. Darmstadt: World Editors Forum.

Rainie, Lee and Janna Anderson (2014): The Future of Privacy. Pew Research. Available at http://www.pewinternet.org/2014/12/18/future-of-privacy/, 18. 4. 2015.

UNESCO (2013): Resolution on internet-related issues. Available at http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/news/37gc_resolution_internet.pdf, 19. 5. 2015.

UNESCO (2014): World Trends in Freedom of Expression and Media Development. Available at: http://unesdoc.unesco.org/images/0022/002270/227025e.pdf, 29. 5. 2015.