Suggestions for privacy-related questions to be included in the list of issues on Kazakhstan, Human Rights Committee, 115th session, October-November 2015

7 August 2015

Main concerns on the right to privacy and communication surveillance in Kazakhstan

Privacy International [PI] is concerned by the broad powers and capacity of security services to conduct surveillance of private communications of individuals in Kazakhstan. In this briefing, PI notes with concern the lack of prior judicial authorisation for surveillance measures; the imposition of obligations onto telecommunication companies to provide security services with direct, unfettered access to their networks; the imposition of mandatory blanket data retention of communication data for two years; the lack of effective, independent oversight; and measures to unlawfully limit the capacity of individuals to communicate anonymously and to express their opinions, as well as seek and receive information, on-line.

I. Kazakhstan's failure to effectively protect privacy and to limit state communications surveillance in its legislation

Article 18 of the Constitution of Kazakhstan (1995) guarantees the right to privacy. The Constitutional protection is reinforced by domestic criminal law: Article 16 of the Kazakhstan Code of Criminal Procedure, which came into force on 1 January 2015, provides for the privacy of "correspondence, telephone conversations, postal telegraph and other communications," and establishes that "[n]o one has the right to collect, keep, use or disseminate information regarding the private life of an individual without his consent, save in cases contemplated by law."[1] Kazakhstan's state report to the Universal Periodic Review provides some figures of crimes against privacy recorded between 2010-2012, including illegal violation of private correspondence.[2]

Covert surveillance and interception of private communications are regulated by the Law on Investigation Activities No. 154-XIII (15 September 1994) and the Criminal Procedure Code. Interception is only permitted for the purposes of detection, prevention and suppression of crimes. It requires a prior warrant by a public prosecutor (notably, not a court). State security services are required to comply with the same criminal procedure regime as the police and other law enforcement agencies.[3]

1 Code of Criminal Procedure of the Republic of Kazakhstan No 231-V (in force from 1 January 2015), Article 16(3).
2 Kazakhstan's second periodic report, UN doc. CCPR/C/KAZ/2, 12 February 2015, paragraph 248.
3 Law of the Republic of Kazakhstan No 527-IV-Z on State Security (6 January 2012).

Under the Law on Communications (No. 567-II of 5 July 2004 and subsequent rules contained in Resolution No. 1593 of 23 December 2011), telecommunication companies (both internet and mobile phone providers) are required to provide organisational and technical assistance to allow state authorities to conduct interception. Article 15 of the Law on Communications requires the companies to put in place equipment to allow the interception of all its subscribers' data.

Counter-terrorism legislation enacted in 2013 grants further broadly defined powers to security services and obliges all mass media (which, under the "Internet Law" adopted in 2009, includes blogs, social media networks and chat rooms) to "assist" in counter-terrorism, without specifying the terms of such assistance.[4]

In law, the procedure to obtain communications data (metadata) is the same as that for the interception of communications (i.e. requiring a public prosecutor warrant).

The Law on Communications requires companies to provide access to all its subscribers' communication data (metadata), including, but not limited, to addresses, e-mail addresses, billing information, subscribers' IP addresses and other relevant information. Further, Article 15.1 of the law imposes a blanket data retention of all subscribers' data for two years.[5]

II. Capabilities of interception by the security services and lack of oversight

The Kazakh telecommunication systems operate within a surveillance model adopted in Russia and other states formerly within the Soviet Union. The System of Operative Investigation Measures (SORM) provides the architecture by which law enforcement and intelligence agencies can obtain direct access to personal data on telecommunications networks, including telephone and mobile networks as well as internet traffic. Unlike American and European frameworks, the SORM model requires direct, unmediated access by law enforcement and intelligence agencies to the communications network.

The companies operating the communications network must install SORM and other surveillance equipment on their networks in order to obtain a license. Once operational, communications over any network operators may be intercepted without the knowledge of the company managing the communication network. Telecommunications companies operating in Kazakhstan informed Privacy International that the government requires companies to install data collection and processing equipment and facilitate direct access for security agencies to such equipment and data.[6]

The capacity of the Kazakh's security agencies to intercept the private communications

4 See Freedom House, Freedom on the Net 2014, page 487.
5 See Telecommunications Industry Dialogue, Provision of real-time lawful interception activities, available here: http://www.telecomindustrydialogue.org/resources/kazakhstan/
6 See Privacy International, Private Interests: Monitoring Central Asia, November 2014.

passing through telecommunications and internet networks is complemented by the use of monitoring centres, wherein the Kazakh government agencies analyse the intercepted data.

According to research conducted by Privacy International in 2014, monitoring centres with mass surveillance capabilities have been provided to Kazakhstan by the Israeli branch of the US-based Verint Systems and by the Israel-based NICE Systems. These monitoring centres are capable of mass interception of telephone, mobile, and IP networks. Such a system means that the communications of every individual are within the reach of the security and law enforcement agencies.

Additionally, Privacy International's research found that Kazakhstan's authorities also rely on distributed monitoring nodes called Punkt Upravlenias (PUs) to manage and access intelligence from smaller segments of the network. Generally, they are are used to intercept the content of communications and communications data (metadata) by collecting and decoding audio communication (such as the sound of telephone conversations), and non-audio communication (such as text messaging or content faxing, etc.) as well as IP data (e-mails, web browser, etc).[7]

While the full range of digital surveillance techniques employed by the security services are unknown, there are reports that sophisticated malware marked by the Italian company Hacking Team is currently or has previously been in use in Kazakhstan.[8] Hacking Team's Remote Control System can be used to hijack computer and mobile devices, whilst remaining undetectable to users, as it is designed to bypass common antivirus programmes and encryption. It can covertly collect, modify and/or extract data from the targeted device, including remotely turning on and control the microphone and camera of the device. As such it is a particularly intrusive form of electronic surveillance given the personal information that can be obtained from such access. The company manufacturing this malware only markets it to law enforcement and intelligence agencies.[9]

These broad, largely unregulated powers are at the hands of security services which are accused of serious human rights violations and which operate without any effective independent oversight of their activities.

Established in 1992, the National Security Committee (KNB) is Kazakhstan's interior intelligence agency and is directly accountable to the President. Its mandate includes

7 For more detailed information, see Privacy International, Private Interests: monitoring Central Asia, November 2014.

8 According to the Hacking Team documents leaked in July 2015, Kazakhstan ranked second in the company's 2015 projected revenues, with a potential revenue of 1.5 million euros (see: http://www.ibtimes.co.uk/hacking-team-hacked-10-things-learned-massive-data-breach-spying-company-1509925).

9 For a briefing on the activities of Hacking Team, see Privacy International, Briefing for the Italian government on Hacking Team's surveillance exports, April 2015, available at: https://www.privacyinternational.org/?q=node/561

counter-espionage, counter-terrorism, and the provision of governmental cryptographic capabilities. It is composed of Joint Chiefs of Staff, national counterintelligence services, the Border Guard, and special purpose military units.[10]

The KNB is heavily involved in the widespread clamping down on legitimate dissent in Kazakhstan. In 2014, the Committee against Torture expressed concerns about the KNB involvement in torture and other ill-treatment for the purpose of obtaining "confession" or information to be used as evidence in criminal proceedings.[11]

The chilling effects of surveillance on the activities of human rights defenders in Kazakhstan have being raised by the UN Special Rapporteur on the rights to freedom of peaceful assembly and association. In the report of his January 2015 visit to Kazakhstan, the Rapporteur reported how at the end of one of his meeting with members of civil society "unknown individuals sitting in the back of a vehicle parked directly facing the entrance of the venue of the meeting were seen taking photographs of the Special Rapporteur's driver and of civil society representatives leaving the building. The equipment used and the manner in which the photographs were being taken left little doubt that the operation was carried out by secret police surveillance with the aim of instilling fear among activists."[12]

There is no independent oversight on the interception of private communications and access to communications data. Articles 24 and 25 of the Law on Investigation Activities provide only for an internal procedure of review to be carried out by the prosecutor, i.e. the same authority that authorises the interception in the first place.

III. Restriction of anonymity and privacy on-line

Kazakhstan has introduced a range of measures aimed at restricting the capacity to communicate anonymously online, as well as conducting wide-scale monitoring of individuals online activities. In a context of widespread repression of legitimate political dissent, such restrictions have a significant chilling effect on the enjoyment of the right to freedom of expression as well as constituting an unlawful interference with the right to privacy. Reports suggest that online activities of some human rights defenders and independent journalists have been monitored and in some cases resulted in arrests and prosecution.[13]

According to the Freedom on the Net report 2014, since early 2011, anonymizing tools,

10 See Security Sector Reform in Central Asia, Erica Marat, The Geneva Centre for the Democratic Control of Armed Forces, 2012, DCAF, available at http://www.dcaf.ch/Publications/Security-Sector-Reform-in-Central-Asia

11 See Committee against Torture, Concluding observations on Kazakhstan, UN doc. CAT/C/KAZ/CO/3, 12 December 2014, paragraph 7.

12 Report of the UN Special Rapporteur on the rights to peaceful assembly and to association, Kazakhstan, UN doc. A/HRC/29/25/Add.2, 16 June 2015, paragraph 14.

13 See Article 19 and PEN International joint submission to the Universal Periodic Review of Kazakhstan, November 2014, available here: https://www.article19.org/resources.php/resource/37576/en/kazakhstan-upr:-article-19-&-pen-international-joint-submission

including proxy sites and specific circumvention software, have increasingly been blocked in Kazakhstan. The UN Special Rapporteur on freedom of expression noted how Kazakhstan has reportedly sought to block Tor traffic (an anonymity tool for internet users), remarking that "because such tools may be the only mechanisms for individuals to exercise freedom of opinion and expression securely, access to them should be protected and promoted."[14]

In 2011, the government introduced further surveillance in cybercafes, requiring cybercafe owners to gather the personal information of customers and retain data about their online activities and browsing history, and to install video surveillance equipment and filtering software.[15]

IV. Proposed questions for the list of issues

Based on these observations, Privacy International proposes the following questions for the List of Issues:

Article 17:

- What measures is Kazakhstan taking to ensure that its state security and intelligence agencies respect the right to privacy?
- In particular, how does Kazakhstan ensure that all interception activities are only carried out on the basis of judicial authorisation and communications interception regime complies with the principles of legality, proportionality and necessity regardless of the nationality or location of individuals whose communications are intercepted?
- What measures is Kazakhstan taking to review its law on retention of communication data (metadata) in order to comply with applicable international human rights standards?
- What measures is Kazakhstan planning to strengthen effective oversight over the surveillance practices of its state security and intelligence agencies?
- How does Kazakhstan ensure that the right to privacy and freedom of expression is respected and protected on-line, including by refraining from limiting access to services that ensure anonymity of on-line users and from targeting individuals for their legitimate exercise of their right to freedom of expression, including to seek and receive information on-line?

14 Report of the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, UN doc. A/HRC/29/32, 22 May 2015, paragraph 52.
15 See Freedom House, Freedom on the Net 2014, page 487.