Nestor Nestor Diculescu Kingston Petersen
ATTORNEYS & COUNSELORS

The Privacy "Challenges" of Cloud Computing

By Roxana Ionescu, Managing Associate,

Head of Privacy Practice

BUCHAREST
Bucharest Business Park
1A Bucharest-Ploiesti Road
Entrance A, 4th Floor
District 1, Bucharest 013681
Romania
T +40 21 201 1200, +40 31 225 3300
F +40 21 201 1210, +40 31 225 3310
E office@nndkp.ro, www.nndkp.ro

TIMISOARA
T +40 256 202 133
F +40 256 202 146
E office.timisoara@nndkp.ro

CLUJ-NAPOCA
T +40 264 433 527, +40 364 229 000
F +40 364 229 005
E office.cluj@nndkp.ro

BRASOV
T +40 268 547 824
F +40 268 547 822
E office.brasov@nndkp.ro

CRAIOVA
T +40 351 228 000
F +40 351 228 005
E office.craiova@nndkp.ro

With cloud computing gaining more and more momentum as compared with the more traditional alternatives for companies to deal with their software applications, data access and storage needs, inevitable questions arise in respect of how such data are actually managed and controlled in a cloud computing environment. One of the most often repeated questions tends to be to what extent providing the data to cloud computing service providers exposes the companies to additional risks of public authorities' interception or may lead to breaches of individuals' privacy rights, especially when the service providers use means located in countries such as the USA, that have in place enactments such as the 2001 USA PATRIOT Act allowing for this type of interception. But when taking a closer look, one cannot help but notice that this is a false issue, as similar interception powers are already set out in the Romanian legislation and, therefore, already apply to the companies' data and communications that would be transferred to the cloud computing service providers.

The right to privacy is one of the fundamental rights set out by the Romanian Constitution. But even constitutional rights cannot be applied in an absolute manner and the Constitution acknowledges that, sometimes, some limitations of or interference with any constitutional right may be required and, therefore, should be allowed. The Constitution also sets forth the main safeguards to be observed. Thus, any interference is to pursue a legitimate purpose, be necessary in a democratic society, be applied without any discrimination and be proportionate to the situation which requires such interference.

These general norms aim at ensuring a fair balance between the fundamental freedoms and rights of individuals, on one hand, and those of the society, on the other, in order neither to undermine nor to destroy the democracy on the grounds for defending it.

Taking this principle further, the Romanian legislation regulates various situations where public authorities' accessing of confidential data or even intercepting communications is allowed. The Romanian Criminal Procedure Code, Law No. 51/1991 on Romania's national safety and Law No. 535/2004 on the prevention and control of terrorism (the latter having a purpose generally similar to the USA PATRIOT Act) all set forth the circumstances when public authorities may intercept communications or gain access to data, as well as the safeguards they need to observe in order to ensure the privacy of such communications or data. While the procedure may vary under each enactment, the following general rules are set forth in all cases:

- any interception of communications or access to date needs to be done for grounded reasons supported by already existing evidence concerning the perpetuation of a criminal offence or by legitimate concerns concerning the perpetuation of serious criminal offences, including drug trafficking, terrorists acts and money laundering;
- as a rule, such reasons are to be assessed and approved by a magistrate (either a judge or, in the case of actions under the laws on national security and fighting terrorism, by specially-designated prosecutors);
- any interception may be carried out only for limited periods of time and are continuously subject to reassessment against the constitutional right to privacy. While the enactments recognize the possibility to prolong the application of the measure, any such prolongation has to be approved under the same conditions as those described above. Moreover, the overall duration of the interception is usually limited to a maximum duration which cannot be surpassed.
- any personal data collected during the interceptions must be protected, including by the public authorities' restricting the access to the such data and implementing additional security measures to protect the data against unauthorized disclosure.

It is true that the Romanian legislator has not been able to strike the right balance between the fundamental rights set by the Constitution and the measures needed to ensure the fight against serious criminal offences in all instances. For example, Law No. 298/2008 on the retention of data generated or processed by suppliers of electronic communication services for the public or of public communication networks, as well as for the amendment of Law No. 506/2004 on the processing of personal data and protection of private life in the sector of electronic communications (adopted in order to transpose the Data Retention Directive 2006/24/EC) was found unconstitutional by the Romanian Constitutional Court in October 2009. In giving this ruling, the Constitutional Court concluded that Law No. 298/2008 introduces rules which interfere with various fundamental rights, including the right to privacy. The Court went on to conclude that such interferences fail to be proportionate and sufficiently clear so as to limit the risk of abuses from the authorities' part. It is to be noted that the Court did not find that the concept of data retention is unacceptable in any circumstances, but that Law No. 298/2008 failed to incorporate sufficient safeguards meant to ensure that the data retention requirements are acceptable by reference to the constitutional rights they may affect, such as the right to privacy.

Similarly to the Romanian framework, the USA PATRIOT Act, which sets forth, amongst others, US authorities' powers to intercept communications and access data, was subject to significant debate and unconstitutional challenges. Nevertheless, at its core, this Act sets forth

the same main interception powers and for the same purposes as those contemplated by the Romanian legislation. Far from allowing unlimited or excessive access to data about individuals, this act provides various statutory limitations that apply to law enforcement agencies' interception actions under the act.

Similar interception rights and under similar conditions are also recognized to authorities in other European Union's member states. In the United Kingdom, authorities' interception powers are provided in the Regulation of Investigatory Powers Act 2000, which also sets the communication areas subject to its provisions (including electronic communications, the Royal Mail and mobile phone networks).

Therefore, whether using their own servers or using cloud computing service providers located domestically or abroad for conducting their activities, companies will always be subject to the possibility of interception of their communication and data. However, such interception is always subject to specific safeguards aimed at striking a balance between the authorities' needs for fighting serious crimes (including terrorism) and the fundamental right to privacy.

******