FINANCIER WORLDWIDE .COM corporatefinanceintelligence

E D I T E D V E R S I O N

This article has been edited to comply with our Editorial Guidelines, which include UK spelling and grammar, and specific house styles for consistency.

RISK & INSURANCE [1625 words]

New EU Directive against cybercrime: the quest for the Golden Fleece?

by Fabrizio Cugia di Sant'Orsola, Chiara Reali and Silvia Giampaolo

Following the echoes of the PRISM scandal and Snowden's revelations, rumours in Europe have it that the so-called 'Article 42' draft new privacy regulation (expected sometime next year) is now to contemplate a further provision, forcing multinational companies to disclose to European data subjects information regarding another country secretly requesting their data.

In parallel, in July, Vice President Viviane Reding announced that the EU Commission would conduct a "solid assessment" of the data protection Safe Harbor programs adopted by the US, given the extent of the scandal, which also affected EU chancelleries.

A fundamental question arises: is there a threat to privacy arising from governmental use of data? Where should the 'iron curtain' of new regulation fall – protecting national boundaries or, rather, individual rights?

Let us assume, for discussion purposes, that foreign governmental access to data may not be denied, for one reason or another. Who commits, then, to non-dissemination obligations?

The fact is that privacy has become an international grey area, and no one knows completely where individual rights effectively start, and with regards to whom such rights prevail.

Cybercrime is an exploding phenomena, costing hundreds of billions of euros every year, according to Catherine Ashton, Security Policy and Vice-President of the European Commission. Yet all this is, if we look at it, the other side of the coin. Cybercrime is a criminal offence worldwide; but on the other hand, and perfectly legal, Big Data – the automatised processing of data by search engines, including pervasive profiling and facial recognition information on data circulating on the web – has irrevocably transformed individual rights.

Data subjects are now mere shadows of former entities protected by law.

Should the evidence of the longing to enact a new EU privacy directive not provide enough proof of the general embarrassment on this issue, a recent opinion of '29WP' (the EU Working Party assisting in the redrafting of privacy regulation) clearly records the difficulty in identifying protective measures in the digitalised world: "additional elements should be included in the data protection regulation in order to provide for a balanced approach on profiling, and mitigate the risks for data subjects. We should identify new transparency measures on operators and increase the data subject power of control" (WP29 Opinion, 13 May 2013). Exactly which 'measures and powers' are of course yet to be seen.

On 19 September 2013, the EU Agency for Network and Information Security (ENISA) reported its analysis of top cyber threats. Cyber criminals increasingly use advanced methods to implement attack vectors, which are non-traceable and difficult to take down. An important role is played by anonymous

technologies and the use of distributed technologies for more 'resilient' infrastructures, such as P2P communications. ENISA observed an increased use of P2P botnets and a rise in TOR-based security measures, while more 'traditional' botnet operations seem to be in decline, due to the low interest in 'traditional' botnet 'business cases'.

Mobile technology is, and will increasingly become, exploited by cyber criminals. Threats of all kinds that were encountered in the more traditional arena of IT will prevail on mobile devices and Over the Top services available on platforms. In addition, the consumerisation of malware, cyber hacking tools and services, together with the availability of digital currencies and anonymous payment services, will open up new avenues for cyber fraud and criminal activity.

ENISA reported on cyber attacks mounted against Spamhouse, leading to noticeable delays for internet users mostly in the UK, Germany and other parts of Western Europe. Spamhaus, based in Geneva and London, is a non-profit organisation which contributes to the fight against spam by providing services enabling operators of email servers to check unsolicited commercial email practices. The attack on Spamhaus was dubbed by online media as the biggest Distributed Denial of Service (DDoS) attack ever seen. In the last stage of the attack, the enormous amount of traffic has caused problems up to switches in the London Internet Exchange, according to ENISA.

On 12 August 2013, the European Parliament and the Council issued Directive 2013/40/EU on attacks against information systems, replacing Council Framework Decision 2005/222/JHA. The Directive establishes minimum rules concerning the definition of criminal offences and sanctions in the area of attacks against information systems. It also aims to facilitate the prevention of such offences and to improve cooperation between judicial and other competent authorities. EU Member States must bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by 4 September 2015, and together with the launch of the European Cybercrime Centre and the adoption of the EU Cyber-security Strategy, the Directive on attacks against information systems should strengthen our overall response to cyber crime and contribute to improve cyber security for all citizens.

Yet cyber security must respect fundamental rights and freedoms as enshrined in the Charter of Fundamental Rights of the European Union, and the topic interfaces with the general Internet Governance ITU regulations and free and open internet policies. This is why the EU did not sign the proposed revised treaty of the International Telecommunications Regulations (ITRs), during the World Conference on International Telecommunications (WCIT) in Dubai on 14 December 2012, due to the risk of the proposed regulation threatening the future of the open internet and internet freedoms, as well as possibly undermining future economic growth.

The Directive introduces the following new elements: (i) penalising the use of offensive tools, such as malicious software like 'botnets', or unlawfully obtained computer passwords; (ii) introducing 'illegal interception' of information systems as a criminal offence; and (iii) improving European criminal justice and police cooperation, including the obligation to collect basic statistical data on cyber crimes. Furthermore, the Directive raises the level of criminal penalties to a maximum term of imprisonment of at least two years. Instigation, aiding, abetting and attempting those offences will become penalised as well. The Directive also raises the level of criminal penalties for offences committed within the framework of a criminal organisation, with a maximum penalty of at least five years, and adds new

aggravating circumstances: (i) when a significant number of information systems have been affected through the use of a tool such as botnets, to a maximum penalty of at least three years;(ii) when causing serious damage, to a maximum penalty of at least five years; and (iii) when committed against a critical infrastructure information system, to a maximum penalty of at least five years.

The Directive does not cover breaches of personal data, but rather systemic cyber attacks that compromise data systems. So, while European institutions are still trying to find an agreement regarding the general data protection regulation, capable of equipping the EU with a set of rules fit for the 21st century on the protection of personal data, the Directive will in parallel ensure that deleting, damaging, deteriorating, altering or suppressing computer data on an information system, or rendering such data inaccessible, intentionally and without right, will be punishable as a criminal offence.

It requires: (i) operators of critical infrastructures who are active in the financial services, transport, energy, health industries; (ii) enablers of information society services such as app stores, e-commerce platforms, internet payment, cloud computing, search engines and social networks; and (iii) public administrations, to adopt risk management practices and report major security incidents on their core services.

In the mind of the EU Commission, this protection is vital to ensure control of data by EU citizens. Such rights stem from Article 8 of the EU's Charter of Fundamental Rights, and privacy is explicitly stated in Article 16 of the Treaty on the Functioning of the European Union. EU Member States, such as Italy, have detailed specific rulings on cyber security and data protection. On 19 March 2013, the Italian Parliament approved decree n. 66 of the President of the Council of Ministers of 24 January 2013, stating new measures to increase online security and protect critical infrastructure from cyber assaults.

Under this Decree, Italy has set up a new government architecture for ensuring national cyber security, defined as "institutional architecture tasked with safeguarding of national security in relation to critical infrastructures and intangible assets, with particular attention to the protection of cyber security and national security, indicating the tasks assigned to each component and the mechanisms and procedures to follow in order to reduce vulnerability, risk prevention, timely response to the attacks and the immediate restoration of the functionality of the systems in the event of crisis" (Article 1).

However, the Decree does not properly address cyber security issues related to private operators, which are as of today exclusively required to: (i) send communications to the Nucleus for Cybersecurity of each and every security or integrity breach of their software systems, using protected broadcast channels; (ii) use best practices as well as cybersecurity measures as defined in Article 16 *bis*, paragraph 1, letter a) of Legislative Decree n. 259/2003 and Article 5, paragraph 3, letter d) of the Decree; (iii) supply information to security information bodies and grant access to the data bank for the purposes of the respective cyber security, in cases provided by Law n. 124/2007; and (iv) cooperate in managing the cybernetic crisis by helping to restore the working order of systems and networks that they manage (Article 11).

There is still a long way to go. And, as in the best of myths, the trophy seems to blur as we move on.

Fabrizio Cugia di Sant'Orsola is a founding partner, and Chiara Reali and Silvia Giampaolo are lawyers, at Cugia Cuomo & Associati. Mr Sant'Orsola can be contacted on +39 06 960 38 103 or by email: f.cugia@cugiacuomo.it. Ms Reali can be contacted on +39 06 960 38 104 or by email:

c.reali@cugiacuomo.it. Ms Giampaolo can be contacted on +39 06 960 38 106 or by email: s.giampaolo@cugiacuomo.it.