CORPO DIGITALE
E
SOVRANITÀ TECNOLOGICA

e-privacy
Firenze
4-5 Aprile 2014

Marco Ciurcina
ciurcina@studiolegale.it

http://it.wikipedia.org/wiki/File:Edward_Snowden-2.jpg

CLOUD & PRIVACY

CLOUD & PRIVACY

United States Director of National Intelligence, James Clapper

"Section 702 is a provision of FISA that is designed to facilitate the acquisition of foreign intelligence information concerning non-U.S. persons located outside the United States. **It cannot be used to intentionally target any U.S. citizen, any other U.S. person, or anyone located within the United States**"

http://en.wikipedia.org/wiki/PRISM_%28surveillance_program%29

E GLI STRANIERI?

PARLAMENTO UE

DIRECTORATE GENERAL FOR INTERNAL POLICIES

POLICY DEPARTMENT C: CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS

The US National Security Agency (NSA) surveillance programmes (PRISM) and Foreign Intelligence Surveillance Act (FISA) activities and their impact on EU citizens' fundamental rights

http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/briefingnote_/briefingnote_en.pdf

PARLAMENTO UE

The US National Security Agency (NSA) surveillance programmes (PRISM) and Foreign Intelligence Surveillance Act (FISA) activities and their impact on EU citizens' fundamental rights

Abstract

In light of the recent PRISM-related revelations, this briefing note analyzes the impact of US surveillance programmes on European citizens' rights. The note explores the scope of surveillance that can be carried out under the US FISA Amendment Act 2008, and related practices of the US authorities which have **very strong implications for EU data sovereignty and the protection of European citizens' rights**.

http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/briefingnote_/briefingnote_en.pdf

PARLAMENTO UE

resolution of 4 July 2013 on the

US National Security Agency surveillance programme,

surveillance bodies in various Member States

and their impact on EU citizens' privacy

http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2013-0322&language=EN

PARLAMENTO UE

resolution of 4 July 2013

Expresses, while confirming its ongoing support for transatlantic efforts in the fight against terrorism and organised crime, serious concern over PRISM and other such programmes, since, should the information available up to now be confirmed, they may entail a **serious violation of the fundamental right of EU citizens** and residents **to privacy** and **data protection**, as well as of the right to **private and family life**, the **confidentiality of communications**, the **presumption of innocence**, **freedom of expression**, **freedom of information**, and the **freedom to conduct business**;

Strongly condemns the spying on EU representations as, should the information available up to now be confirmed, it would imply a serious **violation of the Vienna Convention on Diplomatic Relations**, in addition to its potential impact on transatlantic relations; calls for immediate clarification from the US authorities on the matter;

http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2013-0322&language=EN

PARLAMENTO UE

resolution of 4 July 2013

Calls on the Commission, the Council and the Member States to give consideration to all the instruments at their disposal in discussions and negotiations with the US, at both political and expert level, in order to achieve the above-mentioned objectives, including the **possible suspension of the passenger name record (PNR) and terrorist finance tracking programme (TFTP) agreements**;

Calls on the Commission to conduct a **full review of the Safe Harbour Agreement** in the light of the recent revelations, under Article 3 of that agreement;

Expresses serious concern at the revelations relating to the **alleged surveillance programmes run by Member States, either with the help of the US National Security Agency or unilaterally**; calls on **all the Member States to examine the compatibility of such programmes with EU primary and secondary law**, in particular **Article 16 TFEU on data protection**, and with the **EU's fundamental rights obligations deriving from the ECHR and the constitutional traditions common to the Member States**;

http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2013-0322&language=EN

PARLAMENTO UE

resolution of 4 July 2013

Stresses that all **companies providing services in the EU must comply with EU law without exception and are liable for any breaches**;

Stresses that **companies falling under third-country jurisdiction should provide users located in the EU with a clear and distinguishable warning concerning the possibility of personal data being processed by law enforcement and intelligence agencies following secret orders or injunctions**;

http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2013-0322&language=EN

Rebuilding Trust in EU-US data flows

COM(2013) 846

Communication from the Commission

to the European Parliament and the Council

27.11.2013

Cloud computing:

The proposed regulation includes clear rules on the obligations and liabilities of data processors such as cloud providers, including on security. As the revelations about US intelligence collection programmes have shown, this is critical because these programmes affect data stored in the cloud. Also, **companies providing storage space in the cloud which are asked to provide personal data to foreign authorities will not be able to escape their responsibility** by reference to their status as data processors rather than data controllers.

http://ec.europa.eu/justice/data-protection/files/com_2013_846_en.pdf

Rebuilding Trust in EU-US data flows

COM(2013) 846

Communication from the Commission

to the European Parliament and the Council

27.11.2013

Safe Arbour:

Against this background, a number of policy options can be considered, including:

- Maintaining the status quo;

- Strengthening the Safe Harbour scheme and reviewing its functioning thoroughly;

- Suspending or revoking the Safe Harbour decision.

http://ec.europa.eu/justice/data-protection/files/com_2013_846_en.pdf

Rebuilding Trust in EU-US data flows

COM(2013) 846

Communication from the Commission

to the European Parliament and the Council

27.11.2013

Safe Arbour:

As a matter of urgency, the Commission will engage with the US authorities to discuss the shortcomings identified. **Remedies should be identified by summer 2014 and implemented as soon as possible**.

It is important that the national security exception foreseen by the Safe Harbour Decision is used only to an extent that is strictly necessary or proportionate.

http://ec.europa.eu/justice/data-protection/files/com_2013_846_en.pdf

Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU

COM(2013) 847

Communication from the Commission

to the European Parliament and the Council

27.11.2013

Recommendations

Access by US authorities

12. Privacy policies of self-certified companies should include **information on the extent to which US law allows public authorities to collect and process data transferred under the Safe Harbour**. In particular companies should be encouraged to indicate in their privacy policies when they apply exceptions to the Principles to meet national security, public interest or law enforcement requirements.

13. It is important that the **national security exception foreseen by the Safe Harbour Decision is used only to an extent that is strictly necessary or proportionate**.

http://ec.europa.eu/justice/data-protection/files/com_2013_847_en.pdf

EU-US SUMMIT
JOINT STATEMENT

26.03.2014

12. The transatlantic digital economy is integral to our economic growth, trade and innovation. Cross border data flows are critical to our economic vitality, and to our law enforcement and counterterrorism efforts. We affirm the need to promote **data protection, privacy and free speech** in the digital era while ensuring the **security** of our citizens. This is essential for trust in the online environment.

http://www.whitehouse.gov/the-press-office/2014/03/26/eu-us-summit-joint-statement

EU-US SUMMIT
JOINT STATEMENT

26.03.2014

14. **Data protection and privacy** are to remain an important part of our dialogue. We recall the steps already taken, including the EU-U.S. ad hoc Working Group, and take note of the European Commission Communication of 27 November 2013 and President Obama's speech and Policy Directive of 17 January 2014. We will take further steps in this regard. We are committed to expedite negotiations of a meaningful and comprehensive data protection umbrella agreement for data exchanges in the field of police and judicial cooperation in criminal matters, including terrorism. We reaffirm our commitment in these negotiations to work to resolve the remaining issues, including judicial redress. By ensuring a high level of protection of personal data for citizens on both sides of the Atlantic, this agreement will facilitate transfers of data in this area. The United States and the EU will also boost effectiveness of the Mutual Legal Assistance Agreement – a key channel of cooperation in the digital era. In addition, we are committed to strengthening the Safe Harbour Framework in a comprehensive manner by summer 2014, to ensure data protection and enable trade through increased transparency, effective enforcement and legal certainty when data is transferred for commercial purposes.

EU-US SUMMIT
JOINT STATEMENT

26.03.2014

16. The **Internet** has become a key global infrastructure. We share a commitment to a universal, open, secure, and reliable Internet, based on an inclusive, effective, and transparent multi-stakeholder model of governance. As such, we reaffirm that human rights apply equally online and offline, and we endeavour to strengthen and improve this model while working towards the further globalisation of core Internet institutions with the full involvement of all stakeholders. We look forward to the transition of key Internet domain name functions to the global multi-stakeholder community based on an acceptable proposal that has the community's broad support. We acknowledge the good expert-level cooperation developed in the framework of the EU-US Working Group on Cyber Security and Cybercrime. We commend the political success of our joint initiative to launch a Global Alliance against Child Sexual Abuse Online, as the EU prepares to hand over the lead to the United States, and we decide to tackle jointly the issue of transnational child sex offenders. We reiterate our support for the Budapest Convention on cybercrime, and encourage its ratification and implementation. Building on all these achievements and guided by shared values, we have today decided to launch a comprehensive EU-US cyber dialogue to strengthen and further our cooperation including on various cyber-related foreign policy issues.

SOVRANITÀ

Il Leviatano e le sue “cellule”

hanno lo stesso problema

SOVRANITÀ DELLO STATO

Venezuela, 2002

El golpe petrolero

El rescate del cerebro de PDVSA

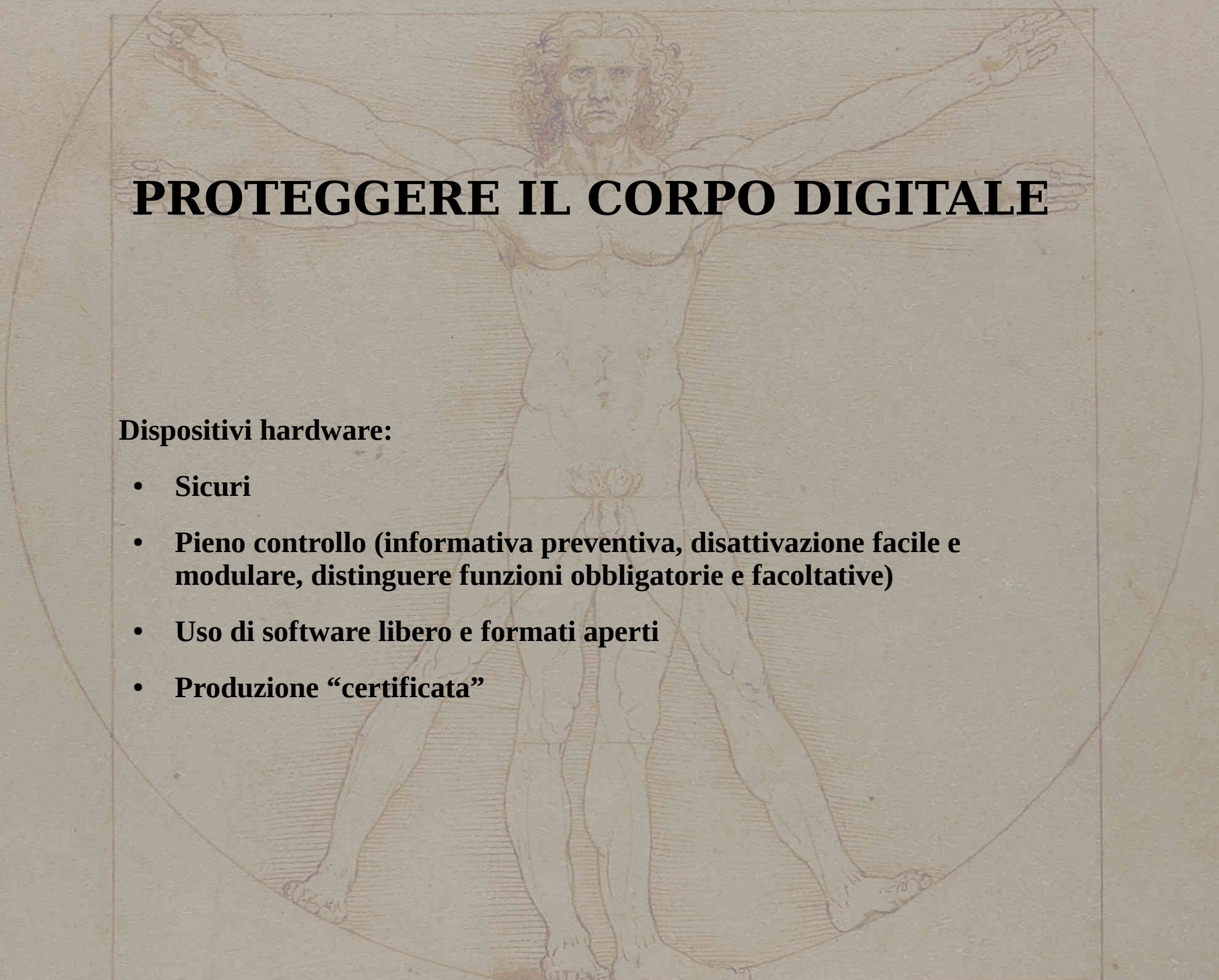
SOVRANITÀ DELLO STATO

Venezuela: Decreto 3.390 sobre el Uso del Software Libre en la Administración Pública (2004) e Ley N° 40.274, de Infogobierno (2013)

Uruguay: Ley n. 19.179 “Software Libre y Formatos Abiertos en el Estado” (2013)

Ecuador: decreto n. 1014 (2008)

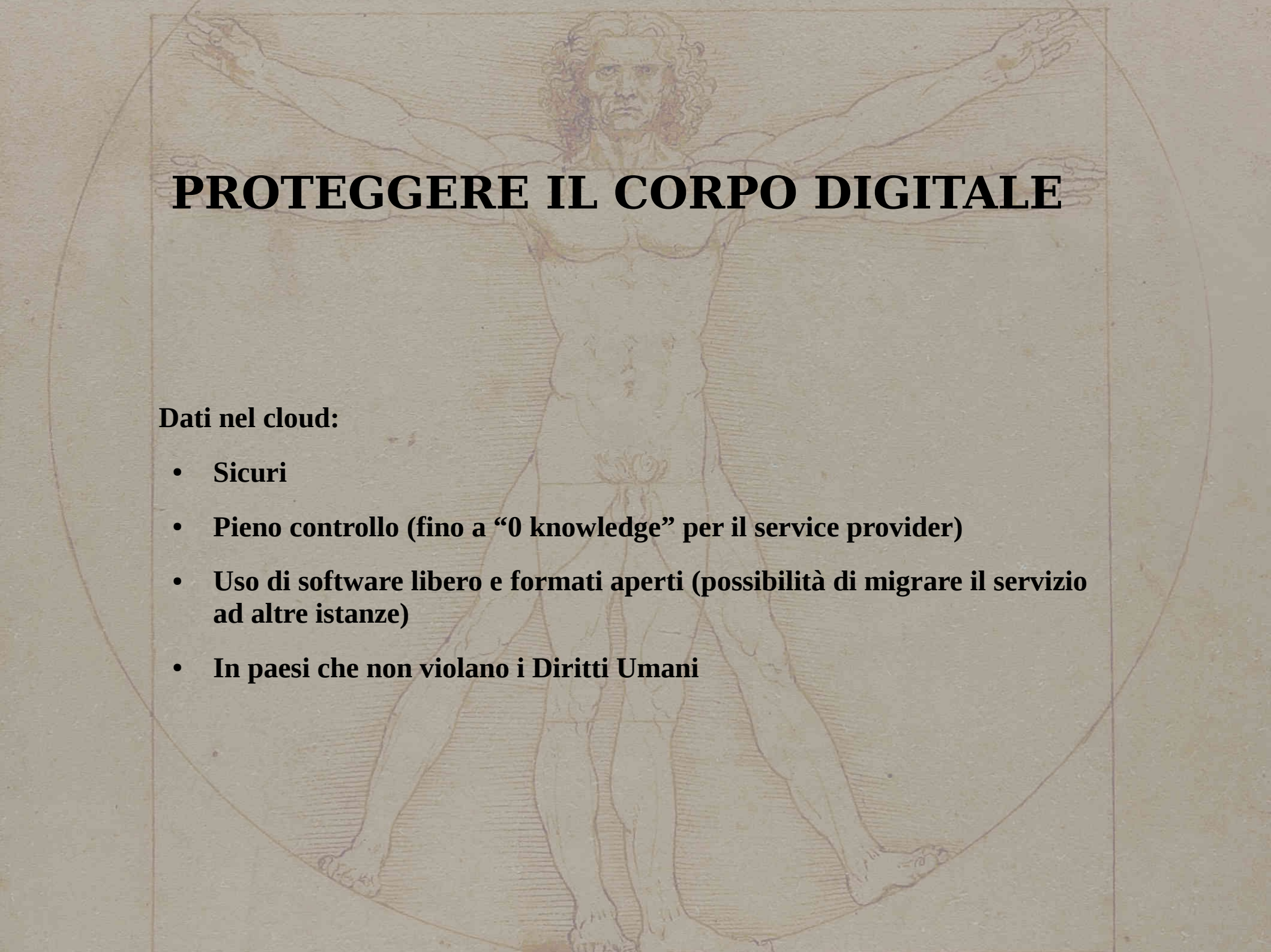
Bolivia: Ley Nro. 164, “Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación” (2011)



PROTEGGERE IL CORPO DIGITALE

Dispositivi hardware:

- **Sicuri**
- **Pieno controllo (informativa preventiva, disattivazione facile e modulare, distinguere funzioni obbligatorie e facoltative)**
- **Uso di software libero e formati aperti**
- **Produzione “certificata”**



PROTEGGERE IL CORPO DIGITALE

Dati nel cloud:

- **Sicuri**
- **Pieno controllo (fino a “0 knowledge” per il service provider)**
- **Uso di software libero e formati aperti (possibilità di migrare il servizio ad altre istanze)**
- **In paesi che non violano i Diritti Umani**

SOFTWARE LIBERO

ADOZIONE

DA PARTE DELLA P.A.

Italian Constitutional Court

N. 122/2010:

I concetti di software libero e di software con codice ispezionabile non sono nozioni concernenti una determinata tecnologia, marca o prodotto, bensì esprimono una caratteristica giuridica

Grazie

ciurcina@studiolegale.it