



Course material

Course:

Understanding the digital supply chain and its stakes for humanitarian actors

Video:

5.2 Rights & obligations vis-a-vis States

Concepts (extracted from automatically generated subtitles):

Organisations' rights. International humanitarian organisations. Service providers. Vis states. Us government. Humanitarian organisations. International organisation. Lawful overseas use of data act. State a. Such agreements. Legal obligations. Cloud act. Criminal proceedings. International organisations. P&i.; p&i.;



[to video sequence search](#)

(within Understanding the digital supply chain and its stakes for humanitarian actors.)



[to video](#)

Center for Digital Education. More educational support material here:

<https://www.epfl.ch/education/educational-initiatives/cede/educational-technologies-gallery/boocs-en/>

page 1/32

CYBERSECURITY

LEGAL CONSIDERATIONS



Rights & Obligations vis-à-vis States

Andrea Raab-Gray

Legal Counsel, International Committee of the Red Cross (ICRC)



...

notes

summary

0m 0s



Rights & Obligations vis-à-vis States



Welcome back. We will now explore organisations' rights and obligations vis-à-vis states. As regards legal obligations, states across the globe are increasingly regulating cyberspace and cybersecurity through legislation and other regulatory frameworks.

notes

summary

0m 4s





Motivations for increase regulation

Strengthening the cyber resilience of critical infrastructure.

Addressing the increasing need for digital evidence in criminal proceedings.

Motivations for increased regulation of cyberspace and cybersecurity are varied. Yet, important drivers for this include ambitions to strengthen the cyber resilience of critical infrastructure and to address the increasing need for authorities to access information in a digital form, for example, to secure digital evidence for criminal proceedings.

notes

summary

0m 23s



European Union's NIS2 Directive



**Objective: Strengthening
the cyber security of
entities that are important
for the states' functioning**

Obligation 1 : Take specific measures
to strengthen cybersecurity.

Obligation 2 : Report certain cyber
incidents to authorities.

The European Union's revised network and information security directive, also called NIS2, is a good example of regulatory action taken to strengthen the cyber resilience of entities that are important for the functioning of a state. This includes, for example, critical infrastructure. Specifically, entities within the scope of NIS2

notes

summary

0m 50s



European Union's NIS2 Directive



**Objective: Strengthening
the cyber security of
entities that are important
for the states' functioning**

Obligation 1 : Take specific measures
to strengthen cybersecurity.

Obligation 2 : Report certain cyber
incidents to authorities.

have two main obligations.

notes

summary

1m 13s



European Union's NIS2 Directive



**Objective: Strengthening
the cyber security of
entities that are important
for the states' functioning**

Obligation 1 : Take specific measures
to strengthen cybersecurity.

Obligation 2 : Report certain cyber
incidents to authorities.

First, they are required to take specific measures to strengthen the cybersecurity, such as adopting policies and ensuring the cyber resilience of their supply chain.

notes

summary

1m 17s



European Union's NIS2 Directive



**Objective: Strengthening
the cyber security of
entities that are important
for the states' functioning**

Obligation 1 : Take specific measures
to strengthen cybersecurity.

Obligation 2 : Report certain cyber
incidents to authorities.

Second, they have to report certain cyber incidents to state authorities. Some international humanitarian organisations might come within the scope of NIS2 and hence be subject to those obligations.

notes

summary

1m 28s





The U.S. CLOUD Act

Purpose

Enacted in 2018, the Act facilitates U.S. authorities' access to data for purpose of criminal proceedings and national security.

Disclosure obligations

Service providers under U.S. jurisdiction must disclose data they control, regardless of its physical storage location, including data stored in other countries.

International Agreements

The Act allows the U.S. government to conclude agreements with other States to directly request service providers to disclose data.

Let's cross the Atlantic now. The US Clarifying Lawful Overseas Use of Data Act,

notes

summary

1m 42s





The U.S. CLOUD Act

Purpose

Enacted in 2018, the Act facilitates U.S. authorities' access to data for purpose of criminal proceedings and national security.

Disclosure obligations

Service providers under U.S. jurisdiction must disclose data they control, regardless of its physical storage location, including data stored in other countries.

International Agreements

The Act allows the U.S. government to conclude agreements with other States to directly request service providers to disclose data.

abbreviated the CLOUD Act, was enacted in March 2018. The CLOUD Act is an important example of legislation intended to facilitate access of state authorities to digital evidence for purposes of criminal proceedings. Specifically, the CLOUD Act enables the US government

notes

summary

1m 52s





The U.S. CLOUD Act

Purpose

Enacted in 2018, the Act facilitates U.S. authorities' access to data for purpose of criminal proceedings and national security.

Disclosure obligations

Service providers under U.S. jurisdiction must disclose data they control, regardless of its physical storage location, including data stored in other countries.

International Agreements

The Act allows the U.S. government to conclude agreements with other States to directly request service providers to disclose data.

to require service providers to disclose customer information relevant for criminal proceedings or national security in two ways. First, the US government can require service providers under US jurisdiction to produce data which the service provider controls, regardless of where it is stored. Even if that data is in another country, what matters is that the service provider is under US Jurisdiction. US jurisdiction is very broad and also captures certain service providers outside the US.

notes

summary

2m 13s





The U.S. CLOUD Act

Purpose

Enacted in 2018, the Act facilitates U.S. authorities' access to data for purpose of criminal proceedings and national security.

Disclosure obligations

Service providers under U.S. jurisdiction must disclose data they control, regardless of its physical storage location, including data stored in other countries.

International Agreements

The Act allows the U.S. government to conclude agreements with other States to directly request service providers to disclose data.

Second, the US CLOUD Act allows the US government to conclude agreements with other states. These agreements typically allow one state party to require service providers in another jurisdiction to disclose certain customer data directly to the requesting state. This is significant, as without such agreements, states would have to resort to so-called mutual legal assistance. This process would be much more complicated. The requesting state could not simply go to the service provider in another state, but they would have to ask the other state to obtain that data

notes

summary

2m 44s





The U.S. has CLOUD Act agreements with the UK and Australia, allowing governments to directly request service providers in the other State to disclose data.

from the service provider, and for that state to then provide the data to the requesting state. Let's turn back to the CLOUD Act. At the time we're recording this,

notes

summary

3m 25s





The U.S. has CLOUD Act agreements with the UK and Australia, allowing governments to directly request service providers in the other State to disclose data.

the US has concluded such agreements with the UK and Australia.

notes

summary

3m 37s





The U.S. has CLOUD Act agreements with the UK and Australia, allowing governments to directly request service providers in the other State to disclose data.

In practice, this means, for instance, that the UK government may require US service providers to disclose certain customer data without going through the US government,

notes

summary

3m 39s





The U.S. has CLOUD Act agreements with the UK and Australia, allowing governments to directly request service providers in the other State to disclose data.

and the US government may require UK service provider to disclose certain customer data without going through the UK government. Importantly, the CLOUD Act does not explicitly exclude data of international or humanitarian organisations from its application.

notes

summary

3m 49s





Impacts for Humanitarian Organizations?

Financial Impacts

Non-compliance e.g. with NIS2 might risk fines and reputational damage.

Confidentiality concerns

Data disclosure could lead to loss of trust, depending on the organization's working modalities.

Particularly, for humanitarian organisations, these legislations might create certain challenges.

notes

summary

4m 8s





Impacts for Humanitarian Organizations?

Financial Impacts

Non-compliance e.g. with NIS2 might risk fines and reputational damage.

Confidentiality concerns

Data disclosure could lead to loss of trust, depending on the organization's working modalities.

For instance, non-compliance with some or all of the obligations contained in NIS2 and similar frameworks may result in hefty financial fines and reputational damage. At the same time, compliance with such obligations might be at odds with the independence of those organisations and the working modalities.

notes

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

summary

.....

.....

.....

.....

.....

4m 15s





Impacts for Humanitarian Organizations?

Financial Impacts

Non-compliance e.g. with NIS2 might risk fines and reputational damage.

Confidentiality concerns

Data disclosure could lead to loss of trust, depending on the organization's working modalities.

Legislations like the CLOUD Act

notes

summary

4m 36s





Impacts for Humanitarian Organizations?

Financial Impacts

Non-compliance e.g. with NIS2 might risk fines and reputational damage.

Confidentiality concerns

Data disclosure could lead to loss of trust, depending on the organization's working modalities.

might result in authorities requiring a service provider to disclose an organisation's data. The CLOUD Act and similar legislation thus illustrate how national legislation

notes

summary

4m 37s





Impacts for Humanitarian Organizations?

Financial Impacts

Non-compliance e.g. with NIS2 might risk fines and reputational damage.

Confidentiality concerns

Data disclosure could lead to loss of trust, depending on the organization's working modalities.

can affect an organisation's cybersecurity, namely the confidentiality and integrity of an organisation's data.

notes

summary

4m 49s





Impacts for Humanitarian Organizations?

Financial Impacts

Non-compliance e.g. with NIS2 might risk fines and reputational damage.

Confidentiality concerns

Data disclosure could lead to loss of trust, depending on the organization's working modalities.

This is particularly problematic for organisations who operate in a confidential manner, meaning that they share certain information only with concerned states and other actors, but not with any third parties or the public at large.

notes

summary

4m 56s





Impacts for Humanitarian Organizations?

Financial Impacts

Non-compliance e.g. with NIS2 might risk fines and reputational damage.

Confidentiality concerns

Data disclosure could lead to loss of trust, depending on the organization's working modalities.

For those organisations, such disclosure could lead to a loss of trust.

notes

summary

5m 10s





Impacts for Humanitarian Organizations?

Financial Impacts

Non-compliance e.g. with NIS2 might risk fines and reputational damage.

Confidentiality concerns

Data disclosure could lead to loss of trust, depending on the organization's working modalities.

States might not trust that the organisation does not take sides and might become reluctant to allow that organisation access to affected people.

notes

summary

5m 16s





Privileges and Immunities granted to International Organizations

Privileges and Immunities (P&I)

- Granted by States through treaties or national legislation.
- Enable independence and efficiency.

P&I usually include

- Immunity from jurisdiction.
- Inviolability of archives.
- Financial privileges.
- Immunity for staff.

Importance

- Managing risks stemming from cybersecurity-related legislations.
- Protection against undue interference BUT not a carte blanche to breach laws.

Consider the following fictitious example. The international organisation, IO, works to improve the situation of children in State A, a state marred by conflict where war crimes are committed frequently. IO uses the services of the service provider SP, which is headquartered in the US. The US has a Cloud Act Agreement with State B, which is a fervent advocate for bringing war criminals to justice and has initiated criminal proceedings against a lead figure in the conflict waging in State A, Mr. Sed, for alleged war crimes. State B understands that IO, in caring for the children of State A, often hears first-hand accounts of children who witnessed war crimes, and saves those files on a platform provided by SP. By virtue of the Cloud Act Agreement with the US, State B might be in a position to request SP to provide IO's data related to Mr. Sed's alleged war crimes for purposes of the criminal proceedings State B initiated against Mr. Sed, irrespective of where that data is stored. The consequences of any such disclosure could be important for IO. Depending on IO's mandate and working modalities, State A might not accept IO's presence any longer, and IO would become unable to serve children in State A. This discussion of the NIS2 Directive and the Cloud Act showcase that it is crucial for organisations to understand the regulatory environment. Which cybersecurity-related legislations apply to them, and what is their impact? How might organisations be impacted through legislations that do not apply to them, but their service or technology providers? Finally, how could these impacts be mitigated? This leads us to the rights which organisations might enjoy vis-à-vis states. Several humanitarian or other organisations are international organisations, such as the ICRC. Where humanitarian or other organisations are also

notes

summary

5m 25s





Privileges and Immunities granted to International Organizations

Privileges and Immunities (P&I)

- Granted by States through treaties or national legislation.
- Enable independence and efficiency.

P&I usually include

- Immunity from jurisdiction.
- Inviolability of archives.
- Financial privileges.
- Immunity for staff.

Importance

- Managing risks stemming from cybersecurity-related legislations.
- Protection against undue interference BUT not a carte blanche to breach laws.

international organisations, they might benefit from privileges and immunities, or P&I.;

notes

summary



Privileges and Immunities granted to International Organizations

Privileges and Immunities (P&I)

- Granted by States through treaties or national legislation.
- Enable independence and efficiency.

P&I usually include

- Immunity from jurisdiction.
- Inviolability of archives.
- Financial privileges.
- Immunity for staff.

Importance

- Managing risks stemming from cybersecurity-related legislations.
- Protection against undue interference
BUT not a carte blanche to breach laws.

P&I; are usually granted by states through treaties or national legislation.

notes

summary

7m 47s





Privileges and Immunities granted to International Organizations

Privileges and Immunities (P&I)

- Granted by States through treaties or national legislation.
- Enable independence and efficiency.

P&I usually include

- Immunity from jurisdiction.
- Inviolability of archives.
- Financial privileges.
- Immunity for staff.

Importance

- Managing risks stemming from cybersecurity-related legislations.
- Protection against undue interference
BUT not a carte blanche to breach laws.

They are legal tools that seek to enable international organisations to carry out their mandates in a manner independent and efficient.

notes

summary

7m 55s





Privileges and Immunities granted to International Organizations

Privileges and Immunities (P&I)

- Granted by States through treaties or national legislation.
- Enable independence and efficiency.

P&I usually include

- Immunity from jurisdiction.
- Inviolability of archives.
- Financial privileges.
- Immunity for staff.

Importance

- Managing risks stemming from cybersecurity-related legislations.
- Protection against undue interference
BUT not a carte blanche to breach laws.

Usually, P&I; granted to international organisations include immunity from jurisdiction, inviolability of the organisation's archives,

notes

summary

8m 2s





Privileges and Immunities granted to International Organizations

Privileges and Immunities (P&I)

- Granted by States through treaties or national legislation.
- Enable independence and efficiency.

P&I usually include

- Immunity from jurisdiction.
- Inviolability of archives.
- Financial privileges.
- Immunity for staff.

Importance

- Managing risks stemming from cybersecurity-related legislations.
- Protection against undue interference
BUT not a carte blanche to breach laws.

financial privileges such as tax exemptions for the organisations, and immunity for the staff of the international organisation. Immunity and inviolability in particular might assist international organisations in managing some of the risks stemming from cyber-related legislations. Inviolability prohibits interference with an international organisation's archives, including data. Immunity, in essence, means that law remains applicable but cannot be enforced against the international organisation. This, of course, does not mean that international organisations have a carte blanche to breach law that in principle applies to them. Indeed, P&I only serve to protect an organisation from undue interference,

notes

summary

8m 13s





Privileges and Immunities granted to International Organizations

Privileges and Immunities (P&I)

- Granted by States through treaties or national legislation.
- Enable independence and efficiency.

P&I usually include

- Immunity from jurisdiction.
- Inviolability of archives.
- Financial privileges.
- Immunity for staff.

Importance

- Managing risks stemming from cybersecurity-related legislations.
- Protection against undue interference
BUT not a carte blanche to breach laws.

but they must not be abused.

notes

summary

8m 58s





In order of appearance

PICTURE1 : Cyber security and information or network protection by Krass99 from Adobe Stock
ICON1: European Union by Ken NL from The Noum Project
PICTURE2 : American Flag by Pasko Maksim from Adobe Stock
PICTURE3 : Justice and Law Concept by Ammy Picca from Adobe Stock
PICTURE4 : International Committee of Red Cross by Kim from Adobe Stock

I hope that after watching this video, you understand obligations and rights toward states in the field of cybersecurity. In the next video, we will look in the direction of the private sector and explore obligations and rights vis-à-vis companies and individuals. After this video, I'd like you to take a minute to reflect on which legislation your organisation might be subject to and how this might impact your organisation. In doing so, please consider your organisation's activities and working modalities.

notes

summary

9m 1s

