Centrum Wiskunde & Informatica

The pseudo-GDPR on digital marketplaces challenge

a general testbed for normative reasoning and GDPR-related applications

11 December 2019, Madrid, GDPR@Jurix workshop

Giovanni Sileno (g.sileno@uva.nl), Thomas van Binsbergen (thomas.van.binsbergen@cwi.nl), Lu-chi Liu, Milen Kebede Girma, Tom van Engers

Background

- The AI & Law field shows that *normative modeling* and normative *reasoning* are far from being solved questions

All legal mechanistic approaches have eventually not been sufficient.

- Some of the reasons for these failures:
  - *vulnerability* to knowledge modularity
  - normative reasoning in some aspects more similar to *analogical reasoning* than *deductive reasoning*.
- …problems very similar to those observed in *common-sense reasoning*!

Background

In limited domains, modularity and structural similarity should not play a role, yet...

- **There is no standard approach to/axiomatization of normative concepts**
  - implicit or explicit deontic logic (regulative dimension)
  - Hohfeldian's framework (regulative and potestative dimension)
  - only power structures [for the operational level]

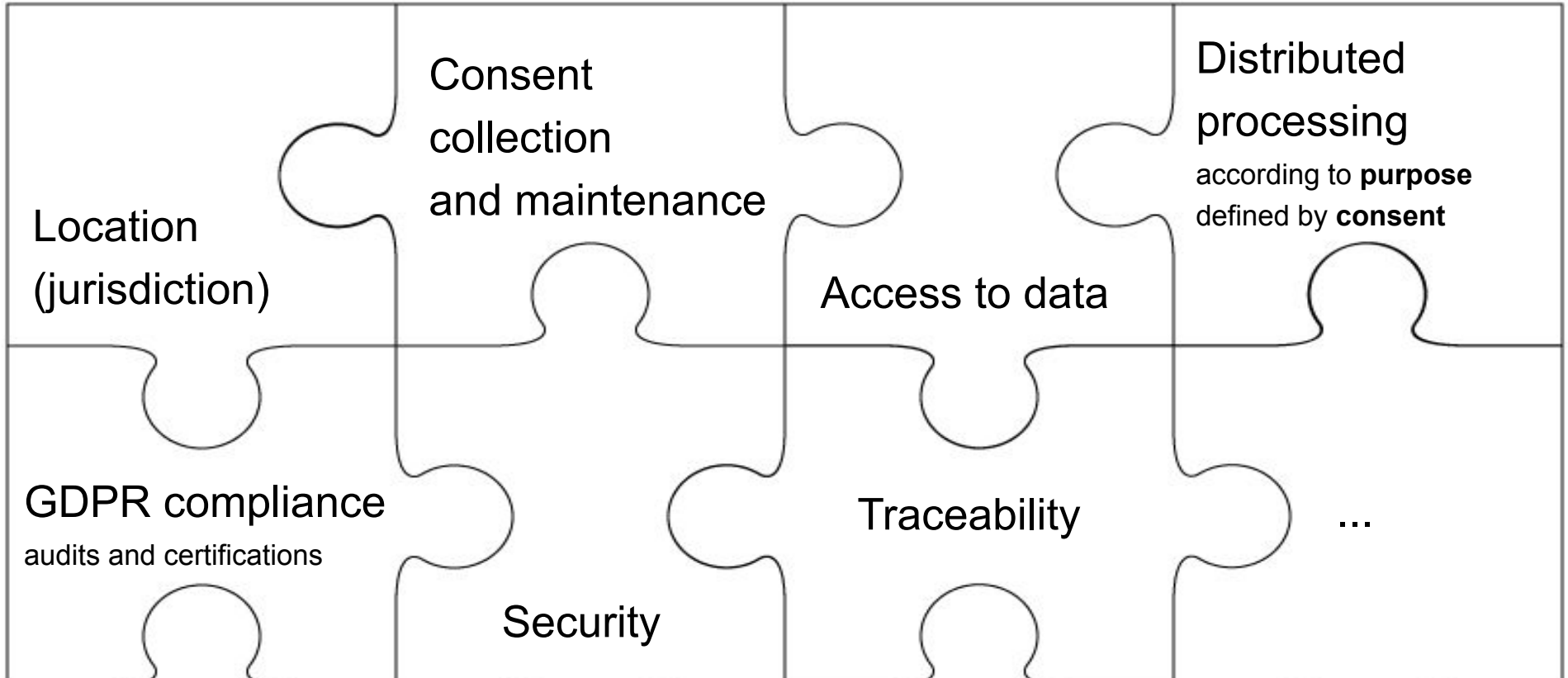
- **No general insight about what is the computational system/technology which is most suitable to perform a certain normative task**
  - best w.r.t. to *validity*, *efficiency*, but also *programmability*, *explainability*, etc.

Setting concrete use cases is a sound strategy for the community to advance.

The GDPR as a sandbox

- The GDPR offers a perfect sandbox. Because it is about data collection and processing, it has strong interactions-with/impact-on computational systems.

Relevant aspects of GDPR

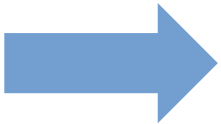


The GDPR as a sandbox

- The GDPR offers a perfect sandbox. Because it is about data collection and processing, it has strong interactions-with/impact-on computational systems.

However, we don't need to consider the actual GDPR to tackle down the issues said before.

- Legal interpretation discussions may distract from "computational" issues.
- We need to emphasize that there is not **"one-fits-all"** interpretation of the GDPR that organizations might directly reuse; they still need to take responsibility, settling upon the actual interpretation they're going to apply.



Our aim is to develop the computational infrastructure in which organizations can encode and use their normative interpretations.

From GDPR to pseudo-GDPR

- The *pseudo-GDPR* is meant to:
  - provide a basic ground, linguistically simpler, to evaluate and compare different axiomatizations (e.g. by forcing modelers to face the ambiguity of the word “right”), languages and reasoners, w.r.t. granularity, clarity, efficiency, programmability, explainability, etc.
  - provide a sufficient normative base to test legitimate uses and non-compliant behaviour (unlawful processing, violation of undue delay of notification or removal of data, violation of satisfying data portability requests, etc.)

Target social domain: *digital market-places* (DMPs)

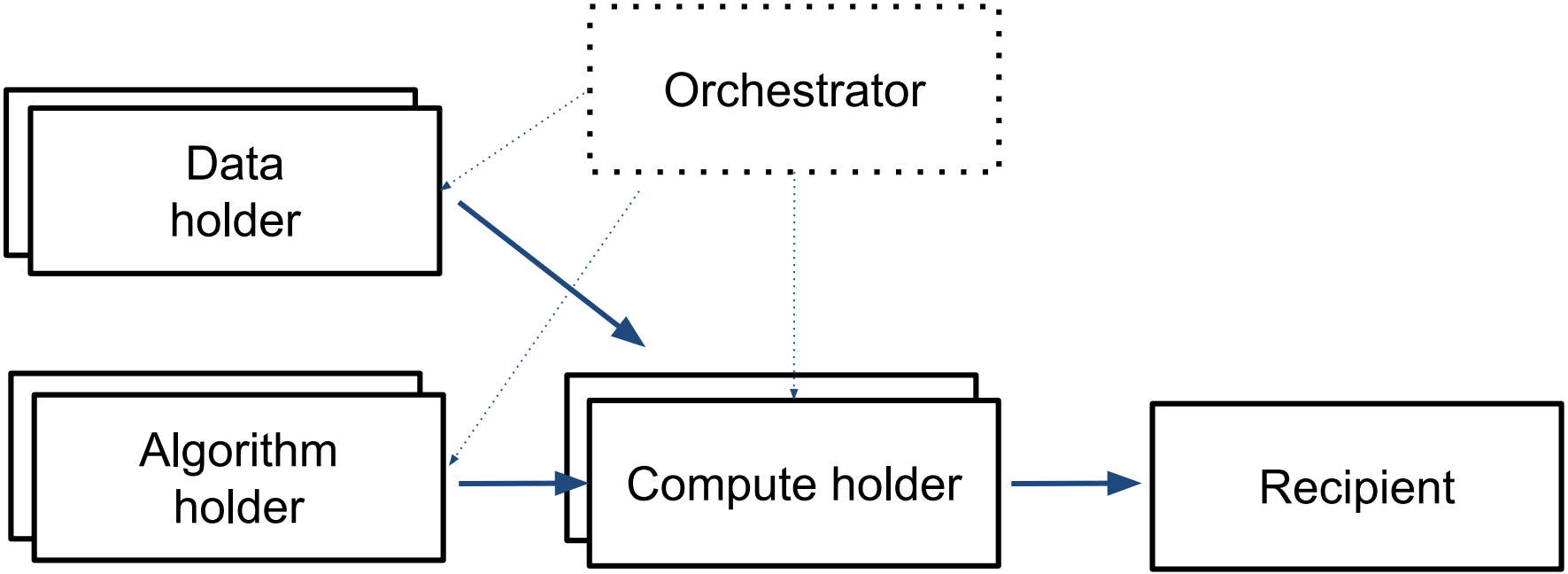
In digital marketplaces, *actors* exchange **data**, **algorithms** and **compute** (computing power).

- some data is ***personal data***: data subjects are included in the DMP as potentially sending data and data-related requests to data controllers
- data controllers are actors interacting with other actors according ***purpose*** (both publicly and privately)

Some actors might be not at arm's length. e.g. a data processor might be structurally connected to an illicit data controller exploiting data.

We need also to capture preferences with DMP (e.g. certain data needs).

General transaction scheme on DMPs



Main roles in GDPR

Data subject

Data controller

responsible of using data according the GDPR and the informed consent given by the data subject

Data processor

responsible for processing data on behalf of the controller

Supervisory authority

Main roles in GDPR

Data subject

Data controller

responsible of using data according the GDPR and the informed consent given by the data subject

Data processor

responsible for processing data on behalf of the controller

Various interactions possible between GDPR roles and DMP roles!

Challenge(s)

Representation

- represent regulations as pseudo-GDPR, consents, and agreements
- represent behavioural domain (scenarios) [w.r.t. DMPs]

Reasoning/Inference

- from given facts, **test**
  - **access-control** (*ex-ante* enforcement)
  - occurrence of **non-compliance** (*ex-post* enforc.) for operational violations and breach of purpose
- provide **explanations** of responses
- given a business process (as a DMP operational description), regulation or agreement, check whether it is **conforming** to pseudo-GDPR

Infrastructural generation

- from use cases and failure cases, place adequate monitoring & responses

Next steps

- Organize working group on the challenge(s)
- Settle down to a definitive version of the pseudo-GDPR
- Settle down an ontology for the DMP social domain
- Identify a number of scenarios of legitimate use and non-compliance
- Identify examples of business processes, consents, agreements, etc.
- Identify sets of event logs containing observations/traces
- Define best/valid responses for the inferential and infrastructural tasks conducted with these components
- Select a method for empirically validating programmability

Are you interested?

- Write us an email!

analysis / visualization

policy-making
interface for
humans

automation

improve the
(digital) governance
of (digital) social systems

computational agents

reference of human agents

PolicyCAD

The policy-cad team

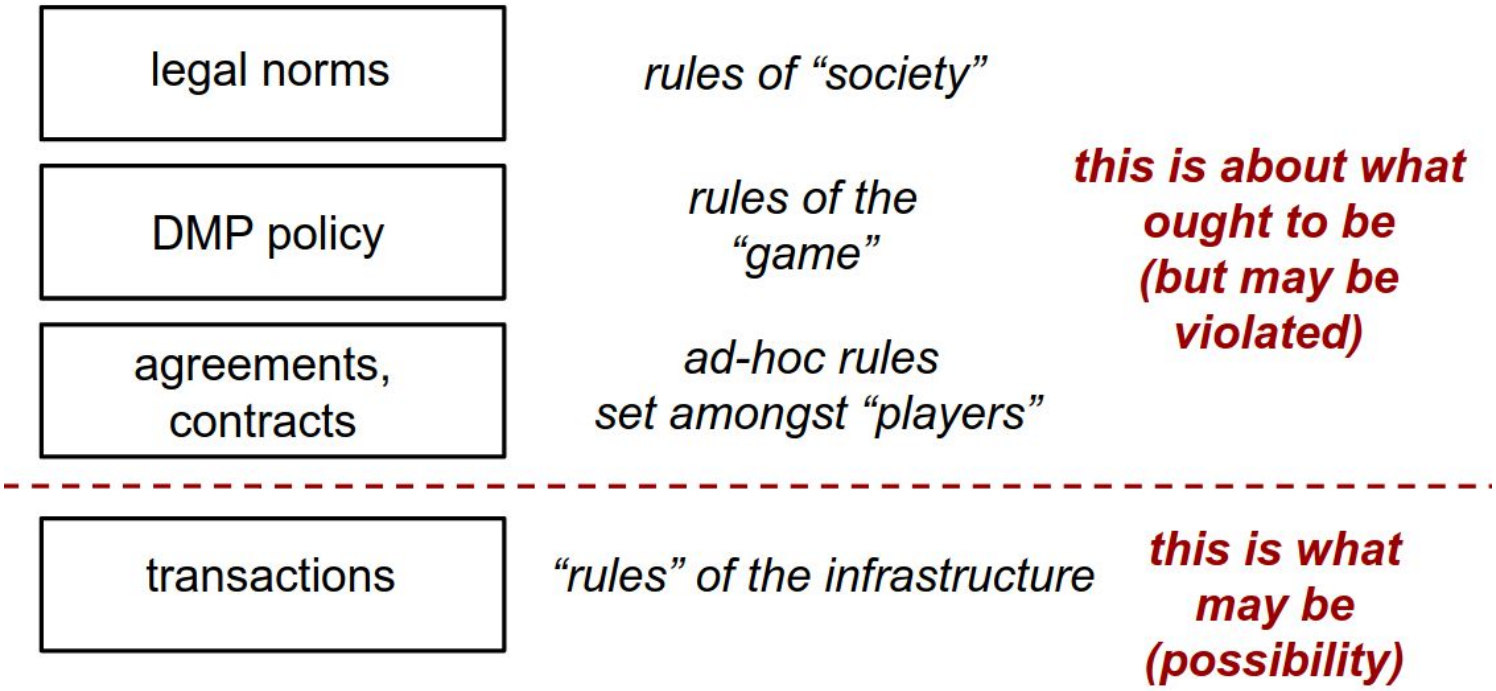
The team is active in several application domains:

- EPI: Data-sharing in health sector
- SSPDDP: Data-sharing between commercial partners
- DL4LD: Data-sharing in logistics
- Agent-programming: Policy aware agent planning/reasoning

Composition:

- 1 professor (Tom van Engers, UvA), 2 post-docs (UvA, CWI), 6+ PhD students (UvA)

Prescriptive characterizations



Centrum Wiskunde & Informatica

The pseudo-GDPR on digital marketplaces challenge

a general testbed for normative reasoning and GDPR-related applications

11 December 2019, Madrid, GDPR@Jurix workshop

Giovanni Sileno (g.sileno@uva.nl), Thomas van Binsbergen (thomas.van.binsbergen@cwi.nl), Lu-chi Liu, Milen Kebede Girma, Tom van Engers

Pseudo-GDPR - 1

pseudo-GDPR applies if data is personal data, data subject is a EU citizen, or data controller or data processor is in EU.

general definitions:

- personal data is any data that can be associated to a physical person
- data subject is any identifiable physical person
- data controller is an actor using data for certain purposes
- data processor is an actor processing data on behalf of the data controller
- personal data processing include collecting, recording, reorganising, storing, modifying, consulting, using, publishing, combining, erasing, and destroying data.

Pseudo-GDPR - 2

data subject has the right:

- to give, modify, and revoke consent to use data for certain purposes to data controller
- to ask to data controller
  - confirmation of whether the controller was processing their personal data;
  - information about the purposes of the processing;
  - information about the fields of data being processed;
  - information about the types of recipients with whom the data may have been shared;
  - a copy of data (in an intelligible) format and the source of data;
  - an explanation of any automated processing that has a relevant effect on data subjects.
- to ask removal of data to data controller

Pseudo-GDPR - 3

data controller has the right:

- [to ask for data subject consent]
- to store personal data from data subject if consent is given
- to use data if this use is compatible with data subject consent

data controller has the duty:

- to modify, remove consent after data subject's request
- to provide to data subject upon request:
  - confirmation of whether the controller was processing their personal data;
  - information about the purposes of the processing;
  - information about the fields of data being processed; ...

Pseudo-GDPR - 4

data controller has the duty:

- to lead removal of data after request
- to refer to pseudo-GDPR-compliant data processors
- to notify data subject of breaches with undue delay
- to maintain a record of data processing activities

data processors has the duty

- [to maintain and remove data after data controller's request]
- to process data only according to the data subject consent
- to notify data controller if consent breach

Pseudo-GDPR - 5

data processor has the duty:

- to delete or return all personal data to the controller after the end of the provision of services relating to processing
- to adequately secure data (encryption, pseudonymization, etc.)
- to notify data controller of breaches with undue delay
- to maintain a record of data processing activities

data processor has the right:

- to use sub-processors after data controller's consent (with full liability)