The *pseudo-GDPR in Digital Market Places* challenge

Giovanni Sileno[1], Thomas van Binsbergen[2], Lu-chi Liu[1], Milen Girma Kebede[1], Tom van Engers[1,3]
[1]*Informatics Institute, University of Amsterdam, the Netherlands*
[2]*Centrum Wiskunde & Informatica (CWI), the Netherlands*
[3]*Leibniz Institute, TNO/University of Amsterdam, the Netherlands*

Motivation

The history of the AI & Law field makes clear that normative modelling and reasoning are far from being solved questions; and that plausibly they will stay open in any case, at least to a certain extent: all legal mechanistic approaches have eventually proven to be not sufficient. We highlight here two of the reasons of these failures: the vulnerability to problems of knowledge modularity, observable also in common-sense reasoning tasks; and the fact that normative reasoning is in many respects more similar to analogical reasoning than deductive reasoning. The two problems have something in common: problems of modularity typically arise when a system of axioms is extended to a domain that was not accounted for at design time; analogical reasoning performs only a partial mapping of the structure of the base domain into the target domain. In both cases, however, if we are within one relatively well-defined domain, problems should not arise.

Yet, there are challenges also in such advantageous conditions. First, there is no standard axiomatization of normative concepts. Most proposals rely on some form of deontic logic (but the continuous introduction of new extensions does not help practitioners to understand which solution is most fitting to their case), some applications refer only to some deontic concepts without a complete axiomatization; other consider additional categories as power (typically following Hohfeld's framework); some others argue that power is, at operational level, what makes the true difference. Furthermore, the fact that laws build on top on common-sense reasoning for aspects concerning the world and the agents, means that some general common-sense ontology is plausibly needed to represent the cases that have to be normatively qualified.

Second, even settling an axiomatization, there is no general insight available to what is the prover/solver or more in general the computational system/technology which is most suitable to perform a certain normative task. "Best" here can be inflected over several dimensions: we should consider not only traditional aspects as validity, and efficiency, but also programmability, explainability, etc. We believe that setting concrete, practical case studies on topics relevant for the whole community is an excellent strategy to face these issues, so we welcome the choice of the organizers to set up this workshop.

From GDPR to pseudo-GDPR

As a matter of fact, 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 believe that it is important to make clear the message, to our community and to the general public that might be interested into these lines of work, that it is incorrect to target one (only?) valid interpretation of the GDPR. Legal experts (and often laymen too) know that the ontological nature of law is much weaker than that of the physical world; parties need to take responsibilities also by settling which interpretation of the law they're going to apply for deciding about their conduct. In other words, organizations should have legal experts complete and refine drafts worked out by the community, but the community cannot

take responsibility for the individual. For this reason, and for the sake of providing a sandbox to investigate the theoretical and technical core issues of the problems stated above, we suggest to consider a simplified version of the GDPR, hereby called the *pseudo-GDPR*.

The pseudo-GDPR is meant to:

- provide a basic ground, linguistically simpler than the original source of law, to evaluate and compare different axiomatizations (e.g. by forcing modelers to face the ambiguity of the word "right") w.r.t. efficiency, programmability, explainability, etc.
- provide a sufficient normative base to test legitimate uses and non-compliant behavior, as e.g. unlawful processing, violation of undue delay of notification or removal of data, violation of satisfying data portability requests, etc.

Application testbed: digital market places (DMPs)

With respect to the social domain on which the pseudo-GDPR should apply, we suggest also to consider a simplified yet relevant view of the world, exploiting the *digital market place* (DMP) concept. In DMPs, actors can exchange *data*, *algorithms* and provide *compute*. To make the GDPR applicable some mechanisms should make in sort that some data can count as personal data, and that data subjects are included in the DMP as potentially sending data, consent and requests to data controllers. Second, data controllers need to operate according purpose (both publicly and privately, to possibly capture non-compliance), therefore some taxonomy of purposes/data couplings is needed to take into account prototypical patterns. Presumably, additional knowledge artifacts has to be added at infrastructural level to make these bridges.

Starting draft of Pseudo-GDPR

For the sake of discussion, we share a starting draft of the pseudo-GDPR, leaving it open to contributions from the community:

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.
2. general definitions:
    a. personal data is any data that can be associated to a physical person
    b. data subject is any identifiable physical person
    c. data controller is an actor using data for certain purposes
    d. data processor is an actor processing data on behalf of the data controller
    e. personal data processing include collecting, recording, reorganising, storing, modifying, consulting, using, publishing, combining, erasing, and destroying data.
3. data subject has the right:
    a. to give, modify, and revoke consent to use data for certain purposes to data controller
    b. to ask to data controller
        i. confirmation of whether the controller was processing their personal data;
        ii. information about the purposes of the processing;
        iii. information about the fields of data being processed;

        iv. information about the types of recipients with whom the data may have been shared;
        v. a copy of data (in an intelligible) format and the source of data;
        vi. an explanation of any automated processing that has a relevant effect on data subjects.
    c. to ask removal of data to data controller
4. data controller has the right:
    a. to ask for data subject consent
    b. to store personal data from data subject if consent is given
    c. to use data if this use is compatible with data subject consent
5. data controller has the duty:
    a. to modify, remove consent after data subject's request
    b. to provide to data subject upon request:
        i. confirmation of whether the controller was processing their personal data;
        ii. information about the purposes of the processing;
        iii. information about the fields of data being processed;
        iv. information about the types of recipients with whom the data may have been shared;
        v. a copy of data (in an intelligible) format and the source of data;
        vi. an explanation of any automated processing that has a relevant effect on data subjects.
    c. to lead removal of data after request
    d. to refer to pseudo-GDPR-compliant data processors
    e. to notify data subject of breaches with undue delay
    f. to maintain a record of data processing activities
6. data processor has the duty:
    a. to maintain and remove data after data controller's request
    b. to process data only according to the data subject consent
    c. to notify data controller if consent breach
    d. to delete or return all personal data to the controller after the end of the provision of services relating to processing
    e. to adequately secure data (encryption, pseudonymization, etc.)
    f. to notify data controller of breaches with undue delay
    g. to maintain a record of data processing activities
7. data processor has the right:
    a. to use sub-processor after data controller's consent (with full liability)

Contacts

If you're interested in joining the working group settling this challenge, please write to g.sileno@uva.nl or thomas.van.binsbergen@cwi.nl.