HOW FAR CAN THE DATA PROTECTION REGULATION GO TO PROTECT AGAINST ALGORITHMIC GROUPS?

DARA HALLINAN
Fraunhofer Institute for Systems and Innovation Research

Image courtesy of dream designs / FreeDigitalPhotos.net

Fraunhofer ISI

Introduction

Current data protection law focuses on protecting individual interests when personal data are processed

However, the focus of processing operations is not always the individual, or their personal data, but the groups to which individuals belong

One type of such group emerges through the analysis of data sets by algorithms

When groups are the focus of processing, data protection law might not always offer a suitable legislative response

The purpose of this presentation is to consider the feasibility of closing this legislative gap by focusing on groups as the target of regulation and to consider how far the Proposed Data Protection Regulation could take us in this direction

1. The problem of algorithmic groups
2. Possible legislative solutions to the group-gap
3. Can groups be a focus of legislation and can algorithmic groups be a focus of legislation?
4. What might legislation aimed at protecting algorithmic groups look like?
5. How far could legislative desiderata could be met by the proposed Regulation?

Fraunhofer ISI

Data Processing, the Group Approach

As ICTs have become powerful, and the data sets they deal with have become larger, new possibilities in processing have arisen

One possibility is for data controllers to use algorithms to analyze large data sets, to identify patterns and ‘types’ within the data set. These types can correspond to groups of individuals.

This processing has consequences:

1. Processing of data relating to groups of individuals can have consequences for each individual member of the group

2. There may be collective consequences which cannot be reduced to the sum of individual consequences

3. There may be broader societal consequences if this type of data processing become commonplace,

Current data protection law does not necessarily offer a satisfactory response to these consequences

1. In processing data on a group, a data controller may not process any ‘personal data‘ relating to any specific ‘data subject’ – law may not even apply

2. Contemporary data protection law was not conceived of with collective harms in mind.

Fraunhofer ISI

Possible Approaches to Fix the Group-Gap

Two possibilities in legislating for the group-gap.

1. Take the individual as the legislative focus:

- The eventual subject of protection is always the individual, even when the group is the focus of processing.
- Further strengthen individual rights in relation to the processing of group data (consider further measures restricting profiling, further measures relating to transparency of group existence and membership, narrower concept of anonymity etc.)

Problems with this approach:

- Reductive: Presumption that dealing with the individual will deal with all problems related to processing of group data
  - Could collective harms be taken into account with a response focused on individual rights?
  - Will individual rights be enough to stop all harms to individuals?

2. Take the group as the legislative focus:

- The focus of processing is the group, so why should a legislative response not also take the group as the relevant unit of reference?

Can Groups be a Focus of Legal Protection?

Yes: International law, constitutional law, corporate law…

Broadly, there are two sorts of groups which are recognized in law. How might we conceptualize algorithmic groups as a focus of law?

1. A group of people as a legal person: The law can recognize anything as a legal entity, groups of people included – corporations, for example

- Used when it is a convenient legal fiction to attribute legal personality to a non-human entity.
- The group as such is seen as a legal entity, with its own rights and obligations separate from those of its individual members.
- Not really applicable to algorithmic groups as a focus of protection

2. The group as a collection of individuals: The individuals share some commonality which constitutes them as a group – religious groups protected by freedom of religion, for example.

- The group is conceived of in terms of the collective set of rights and relationships of its members
- Concept of a collective group fits quite well with algorithmic groups as a focus for legislation
- So, are algorithmic groups reducible to the typical collective group protected in law?

Fraunhofer ISI

Can Algorithmic Groups be Collective Groups? Characteristics (1)

Traditional collective groups recognized by law tend to:

- Have some level of organizational structure
- Have common awareness – members are aware of their membership and of other members' membership
- Have a shared goal/identity
- Have a certain stability of membership

Algorithmic groups depart from this model

- Groups may only recognizable from their creator's perspective
- Unlikely to have 'independent' organization or organizational structure
- Unlikely to have 'independent' goals
- Members may be unaware of the existence of the group, their membership of the group or the identities of other members
- Membership may change quickly and unpredictably as the algorithms defining the group change

Difference in characteristics of groups not an obstruction to conceptualizing algorithmic groups as a focus of legislation, but will be of considerable importance in considering how legislation might look

Fraunhofer ISI

Can Algorithmic Groups be Collective Groups? Justification for Protection (2)

Traditional collective groups are the focus of legislation for a number of reasons:

1. The groups themselves are seen as having systemic value and therefore should be protected – religious groups are seen as 'indispensable for pluralism in a democratic society'

Does not apply to algorithmic groups

- The groups themselves may only be valuable to the creator. Their existence is unlikely to be regarded as having social value.

2. The existence of the group needs to be protected in order for individuals to enjoy their rights cannot enjoy their rights – the existence of a religious group provides the vehicle within which individual rights can be enjoyed

Does not apply to algorithmic groups

- The existence of an algorithmic group is not a prerequisite to allow the enjoyment of rights

3. Regulation on the level of the group needs to be there to prevent adverse consequences for individual members of that group or to prevent unfair treatment of the members of the group – non-discrimination legislation

This final justification applies well to algorithmic groups

Fraunhofer ISI

What Might be Desirable in Legislation for Algorithmic Groups?

Context is one of factual uncertainty but perceived risk. First step is to gather the relevant information – what is the scope of the issue, what harms are really being caused, which benefits are being created etc.

- *Ex ante* mechanisms aimed at making processing related to algorithmic groups transparent – collecting factual and risk information
- *Ex ante* control mechanisms for checking on, and preventing, in advance, disproportionately harmful processing
- Prohibitive provisions without base factual information would be legislative overkill

Guidelines elaborating when processing related to such groups is legitimate and guidelines elaborating how group data should be dealt with

Ex post compliance checking and sanctions if legislation were to be ignored

Wouldn't want to give group algorithmic groups actionable rights, or make the group responsible in any way – who would be responsible? Where would their legitimacy come from? What would the rights be, and how would they be reconciled with individual rights in a conflict?

Any approach focused on algorithmic groups should not be prejudicial to pre-existing individual rights

If algorithmic groups cannot be responsible for their own protection, then there would be the need for an independent body tasked with this function – including reception and evaluation of information, exercising judgment and prohibiting harmful processing and pursuing sanctions

How close does the Proposed Data Protection Regulation come to fulfilling these desiderata? With some minor changes, actually quite close

Fraunhofer ISI

The Data Protection Regulation (Scope)

Applies only when ‘personal data’ of a ‘data subject’ are processed.

- Will not apply if algorithmic groups emerge from data sets not composed of personal data.
- Algorithmic groups themselves cannot qualify as ‘data subjects‘ according to Article 4(1) - a data subject must be a natural person

This is not an insurmountable obstacle. 2 Options:

1. Extend the current concepts of ‘data subject’ and ‘personal data’ to include groups. This would raise significant complications

- The concept of data subject is tightly tied to system of active rights and obligations – do not want to give algorithmic groups active rights
- This would put groups and individuals on a par - this would lead to interest conflicts between the group and the individual

2. Elaborate an additional concept which extends the scope of the Regulation – group data subject, group data etc.

- This would avoid the problematic connotations of current concepts

Fraunhofer ISI

The Data Protection Regulation (Advance Checking)

The Regulation includes *ex ante* checking and control mechanisms

Article 33 outlines the necessity of conducting a Data Protection Impact Assessment in a number of situations. This would be an ideal mechanism for the production of factual, and risk information relating to processing of algorithmic groups.

- The situations currently listed would not necessarily include processing of data on algorithmic groups, but this list could be easily amended
- There is no reason a DPIA methodology could not be applied to consider the risks of processing done on algorithmic groups (SAPIENT Project).
- Evaluating the risks of processing involving algorithmic groups through a DPIA need not be prejudicial to individual interests

Article 34(2) states that processing operations subject to an impact assessment are subject to a DPA's prior consultation and authorization.

- The inclusion of processing on algorithmic groups as requiring an impact assessment would mean prior approval would be required from the DPA before processing could happen.
- Prior checking and approval would function as a mechanism to prevent disproportionately harmful processing in advance

Fraunhofer ISI

The Data Protection Regulation (Legitimation and Processing Principles)

Articles 6 and 9 lay down criteria for lawful processing

- Consent is irrelevant as a ground for legitimate processing for algorithmic groups (who would give their consent?)
- Other exceptions, not related to individual rights, could be functional – e.g. public interest, legitimate interest of the controller etc.

Articles 5, 22, 30, 35 etc. lay down technical, organizational and procedural obligations on data controllers related to the fair treatment of data

- Most of these obligations could be applied to groups – e.g. purpose limitation, data security, privacy by design etc.
- These are seldom attached to any single, or any specific concept of, rights holder
- Obligations should normally be fulfillable in relation to both groups and individuals at the same time

Fraunhofer ISI

The Data Protection Regulation (Compliance and Sanctions)

Article 52 elaborates the power of the supervisory authority (DPA) to

- 'monitor and ensure the application of the Regulation' (52(1)(a))
- 'conduct investigations on its own initiative [into processing operations]'

Article 76 outlines the power of the DPA to instigate court proceedings

Articles 53 and 79 outline sanctions for failure to comply with the provisions of the Regulation

- Article 53 includes a number of remedial sanctions – e.g. demanding rectification of problematic processing, freezing processing, banning processing etc.
- Article 79 outlines financial sanctions

If the scope of the Regulation were extended to processing on algorithmic groups, and obligations were to apply when group data is processed, DPAs are ideally placed to perform *ex post* checking and sanctioning with existing powers

Problems with Extending Protection to Algorithmic Groups

Definitions and details:

- How would algorithmic groups be defined?
- Which algorithmic groups should be included in the scope of the Regulation?
- How would it be established which data related to these group etc.?

Adequacy and suitability of existing provisions: Simply as existing provisions could be extended to groups and even without interfering with individual rights, does not make such provisions ideal for regulating processing of group data

- Certain obligations and processing principles would be applicable but only with different sets of supporting considerations – e.g. What would the accuracy of data related to an algorithmic group mean (the accuracy of the judgment of that group, the accuracy of the initial data etc.)
- If thought were given to a set of controller obligations and processing principles for group processing, would they be the same as those in the current Regulation?
- Data protection law alone is unlikely to be able to completely provide a legislative response

Interest conflicts: The extension of the Regulation to groups would not directly pit group against individual, nevertheless interest conflicts would be inevitable – e.g. If consented to processing on an individual level were halted based on concerns related to the group

- How would such conflicts be resolved?

Fraunhofer ISI