Deception by design?

Speech to ISMS Forum Spain: XXI International Information Security Conference, Madrid

30 May 2019

Giovanni Buttarelli

Ante todos, muchas gracias por la invitación a dar esta breve intervención.

I was pleased - and a little curious - when Daniel Garcia Sanchez asked me to share some reflections on the theme of 'deceived by design'.

This is a provocative title.

Because, as you know, one of the innovations of the GDPR is 'data protection by design'.

Article 35 of the GDPR creates a legal obligation on the controller to implement data protection principles from the moment he or she decides to process personal information.

The Article explicitly refers to data minimisation as an example of one of these principles.

You can read our recommendations on putting this article into practice in our preliminary opinion published exactly year ago, in May 2018.

It is also almost exactly a year since the GDPR became fully applicable.

You in this room, as DPOs and CISO, will understand better than anyone the efforts that have been necessary to ensure compliance with the GDPR.

Reviewing the data practices of an entire organisation is a big and complex task.

The GDPR is very prescriptive of the obligations on controllers and also processors.

But it is not a handbook, and it promotes the notion of accountability. This means that controllers should not be 'spoon fed' by the regulator or to supervisory authority.

Instead, the controller should be critically aware of the data processing which the organisation relies on, and take responsibility when something goes wrong.

The controller should reflect honestly on the interests of the people whose data are being processed.

From the outside, however, in the experience of most people, it is not clear what has changed in the last year.

Has the GDPR actually changed our digital lives?

Do we have more confidence that data about us is being treated fairly, respectfully and safely?

Has data minimisation and privacy by design suddenly become the norm.

You might have guessed that these are largely rhetorical questions.

The GDPR was ambitious but it was never going to transform business models overnight.

But if I am honest, I have been disappointed by the response of many companies since May 2018.

When I think of the thousands of emails and popups which tell me that I must click and accept the terms of service - the impression is that the first priority has been to preserve the old way of doing things.

Then of course there are the many scandals of the past 18 months, of which Facebook/ Cambridge Analytica is only the highest profile.

The data of millions has been compromised.

It is claimed that these are 'bugs' in the system.

But the suspicion is that this is collateral damage for a business model which relies on constant tracking of people - data maximisation, in other words.

As a result, data protection authorities in Europe have never been busier.

This week the EDPB will publish the latest statistics on the number of cases being handled by individual DPAs including cross border cases in the one stop shop.

Already, in March, there were over 255 000 national cases, and almost 1000 cross border cases.

Among these cases are very high profile complaints that challenge the entire behavioural advertising ecosystem, and the legal basis of processing by the biggest social media companies in the world.

And for people who try to access data held about them by big companies, the process is often difficult and the outcome less than satisfying.

This corroborates the findings of surveys and reports around the world – whether in Europe, the US, or even China - that trust in providers of online services is very low, unfortunately.

People are beginning to appreciate the gap between the marketing slogans and the reality.

So, is the reality "deception by design"?

Let us take a step back.

It is human nature to enter exchanges with the aim of getting more than you are prepared to offer in return.

In that sense, inequality is a fact of life.

There comes a point however where power imbalances become both unjustifiable and unsustainable.

Regulation has evolved to try to tackle this - regulations like the GDPR but also consumer protection, product safety standards and antitrust.

Periods of rapid technological change tend to increase these imbalances.

The disparity constantly grows between those who have control of the technology, and those who are the objects of the deployment of that technology.

This helps explain why, in the last two years people have begun to speak of manipulation and exploitation.

I mentioned the emails and popups that clearly aim to nudge or bully people into accepting non-negotiable 'privacy' policies.

A typical defence from companies is that they are just giving people what they want.

People expect free services, and is only possible if their behaviour can be monitored and monetised.

But if people realised the actual value exchange, they would probably expect a lot more in return than they are getting.

You see this in trivial circumstances, like when you are considering renting a car or a booking a hotel.

If you take your time, you start to see warning messages -

Hurry up! 10 other people are looking at this hotel. Or

Don't wait until it's too late! Don't lose today's saving.

Is this sincere? How can we know?

eCommerce sites try to panic you into making a purchase, and place 'important information' about the terms and conditions on parts of the screen which you are less likely to see.

The Norwegian Consumer Council last year published a detailed study into the 'dark patterns' which try to seduce you into accepting the data practices which are in the interests of the service provider.

They tempt you to click the cool blue 'accept' button, instead of the grey and tedious 'manage settings' alternative.

Is any of this illegal?

Possibly, but not necessarily.

Such practices will be tested in the courts in the coming years.

But it is disappointing that we have to wait for litigation.

Europe instead should be innovating in ways that will enable businesses to earn the trust of people again.

A first step would be to reconsider what we mean by consent.

Consent has to be specific, informed and freely given.

If what you are doing with data is clearly unobjectionable – maybe consent is not the appropriate legal basis.

You should be confident that you have risk mitigation measures in place, that you are considering the best interests of the individual data subject, therefore aim to rely on the legitimate interests legal grounds.

My prediction is that as the GDPR beds in, and as the rest of the world increasingly emulates Europe's standards, we will see some new business models emerge – where data protection by design is visibly in play.

It will be up to regulators and supervisory authorities to support such innovation.

Thank you for your attention, and my best wishes from Brussels for a successful day of discussions.