UK data protection watchdog intends to impose maximum fine on Facebook

LNB News 11/07/2018 117

The information Commissioner's Office (ICO) has published two reports detailing its investigation into the use of data analytics in political campaigns. The first report includes proposals to fine Facebook £500,000—the maximum allowed—for two alleged breaches of the Data Protection Act 1998 (DPA 1998), while the other includes a recommendation for the government to introduce a statutory Code of Practice for the use of personal data in political campaigns. Ian Wilson, partner at Brett Wilson LLP and Dr Mark Leiser, lecturer in law at the University of Leicester highlight the reputational damage the proposed fine has for Facebook, whereas Dan Whitehead, senior associate at Kemp Little, demonstrates how the report reveals the complexity of the data sharing networks that now exist between public and private sector organisations. James Seadon, partner at Fieldfisher, draws on the report's broader implications, while Professor Steve Speers at the University of Essex, argues that data protection law—as well as electoral law—need a 'complete overhaul' if they are to keep abreast of the pace of change set by social media. And Danielle Amor, senior associate at Pannone Corporate, warns that, in the age of big data, it is not just social media companies who need to pay heed to the example the ICO has made of Facebook.

In March 2017, the ICO began examining the use—and potential misuse—of personal data by campaigns on both sides of the EU referendum. In May 2017, it widened its scope, launching a further investigation into political parties, data analytics companies and major social media platforms.

The progress report provides details of some of the organisations and individuals currently under investigation. These include:

• 29 other social media companies

• political campaign groups

• political parties

• other commercial actors

Dan Whitehead, senior associate at Kemp Little, highlights that the 'breadth of the investigation provides a useful illustration of the complex nature of the data sharing networks that have been established between both public and private sector organisations. It should also serve as a warning to companies who seek to either share with or purchase personal data from third parties about the potentially high regulatory risks of doing so'.

For example, the report alleges that a data analytics firm, Aggregate IQ—which worked with Vote Leave during the EU referendum campaign, itself chaired by prominent politicians, such as Michael Gove and Boris Johnson—had access to UK voters' personal data. The ICO is now investigating whether this information was transferred and accessed outside the UK and whether this amounted to a breach of DPA 1998.

With regards to the ICO's investigation of Facebook, Ian Wilson, partner at Brett Wilson LLP, highlights that 'at all material times the governing law was DPA 1998, which imposed a number of obligations on data controllers known as "Data Protection Principles". These include requirements to process personal data fairly and to have appropriate technical measures in place to ensure that personal data is secure—respectively, the first and seventh Data Protection Principles. These are the obligations Facebook is said to have breached'.

Since February 2018, Facebook—alongside the data analytics firm Cambridge Analytica (CA)—has been the focus of the ongoing investigation after evidence emerged that a third-party app was used by CA to harvest the data of 87m unwitting Facebook users across the world.

The ICO's investigation concluded that Facebook 'contravened the law by failing to safeguard people's information'. It also found that the company 'failed to be transparent about how people's data was harvested by others', such as CA.

The ICO also plans to bring criminal actions against CA's now defunct parent company, SCL elections.

'At a crossroads'

'We are at a crossroads,' said information commissioner, Elizabeth Denham in a statement. 'Trust and confidence in the integrity of our democratic processes risk being disrupted because the average voter has little idea of what is going on behind the scenes.

'New technologies that use data analytics to micro-target people give campaign groups the ability to connect with individual voters. But this cannot be at the expense of transparency, fairness and compliance with the law'.

'Bad actors'

The ICO has issued a Notice of Intent to fine Facebook £500,000 for alleged data breaches—the maximum possible under DPA 1998.

'Fines and prosecutions punish the bad actors, but my real goal is to effect change and restore trust and confidence in our democratic system', claimed Denham.

However, as Wilson illustrates, Facebook's fine is relatively small compared to those than can be imposed under the General Data Protection Regulation (GPDR):

'Facebook should be grateful that these breaches occurred under DPA 1998. DPA 1998 has now been repealed and replaced by the GPDR and Data Protection Act 2018 (DPA 2018). The maximum sanction for breaches under the new legislation is €20m (£17.7m) or 4% of annual global turnover, whichever figure is higher. In Facebook's case, this could mean a fine of over $1.6bn (£1.2bn).

'While some might say Facebook has got off lightly here, the exposure of the breach and the ICO's sanction will inevitably damage Facebook's reputation as it diminishes trust in the platform amongst users'.

Dr Mark Leiser, lecturer in law at the University of Leicester, echoes this notion of reputational damage outweighing the fine for Facebook, claiming that 'this will be seen as a political event as much as a data protection one. And although one outcome might see Facebook making representations to the ICO that result in the fine reduced to nothing, I don't suspect Facebook will be sending the ICO any friend requests any time soon'.

James Seadon, partner at Fieldfisher, builds on this insight, highlighting the 'broader implications' of the ICO's Notice of Intent:

'The Commissioner's statement signals her close interest in the broader data sharing economy. And her decision to publish the Notice of Intent—something that is normally kept private until the fine itself is levied—reflects not only the substantial public interest in this matter but also the ongoing political scrutiny'.

Facebook has a chance to respond to the Commissioner's Notice of Intent, after which a final decision will be made.

'Democracy disrupted?'

The ICO also published a second, partner report entitled 'Democracy disrupted? Personal information and political influence', which outlines the findings and recommendations arising out of the 14-month investigation.

Among the ten recommendations is a call for the government to introduce a statutory Code of Practice under the DPA 2018 for the use of personal data in political campaigns. The ICO has volunteered to work closely with the government to determine the scope of the code.

The report also stressed the need for an 'ethical pause' to allow government, parliament, regulators, political parties, online platforms and the public to 'reflect on their collective responsibilities in the era of big data before there is a greater expansion in the use of new technologies'.

Professor Steve Speers at the University of Essex concurs with this notion, claiming that a 'complete overhaul is necessary to ensure that limits on spending, foreign interference and unaccountable dishonesty in elections are effectively enforced'.

The ICO said it expects the next stage of its investigation to be complete by the end of October 2018.

'Serious sanctions'

However, Danielle Munro, senior associate at Pannone Corporate, warns that, in the age of big data, other global businesses should pay heed to the example the ICO has made of Facebook:

'Social media platforms and political parties and campaigns are clearly high on the ICO's current agenda, but other global businesses ought to take note too. Failure to provide sufficient information to individuals, to properly safeguard personal data and to take prompt and effective measures in response to a data breach are all likely to attract serious sanctions for data controllers in future'.

Source: Report: Findings, recommendations and actions from ICO investigation into data analytics in political campaigns