GDPR and the Computer Misuse Act – Corporates Beware

Related Lawyers:

Related Practice Areas: **Technology Disputes**, **Commercial Disputes**

Historically, the Computer Misuse Act 1990 (the Act) has been used, as one might expect, in cases concerning computer misuse such as computer hacking or industrial terrorism. More recently, however, the Act has been applied more widely to prosecute instances of data misuse. In the era of significant financial penalties under the GDPR, the added prospect of criminal sanctions under the Act should lead corporates to take particular care to ensure data is obtained from computer systems in an authorized manner. Conversely, in light of COVID-19 with reports of fraudsters taking advantage of the situation to commit cyber-crimes, the added layer of recourse may act as a welcome safety blanket.

Offences under the Computer Misuse Act

Amongst other provisions, the Act covers four criminal offences:

1. unauthorised access to a computer system with intent to commit or facilitate the commission of further offences (for example, theft, blackmail or fraud)
2. unauthorised acts with intent to impair, or recklessness as to impairing, the operation of a computer system
3. unauthorised acts in relation to causing, or creating a significant risk of, serious damage of a material kind to a computer system
4. making, supplying or obtaining articles for use or to assist in the commission of any of the above offences.

The Act's provisions are expansive: they do not draw a distinction between 'data' and 'personal data' as does the GDPR. The key factor in determining whether an offence has been committed is the misuse of a computer system in itself. This contrasts with the GDPR where the key factor is the type of data that has been accessed.

Evolving approach

Traditionally, the Act was used to criminalise plainly criminal acts relating to the misuse of computer systems. More recently, however, it has been used to criminalise the unauthorised access of personal data by a business with a view to furthering its commercial interests.

In *R. (on the application of Pensions Regulator) v Workchain Limited* [2019] EWCA Crim 1422, the Pensions Regulator succeeded in bringing criminal proceedings against employment agency Workchain and its directors under the Act. The proceedings concerned Workchain's unauthorised obtaining of confidential pensions data held by the National Employment Saving Trust relating to its work force with the aim of opting its workers out of workplace pensions, thereby saving Workchain the requirement to make pension contributions.

Commentary

Whilst it is likely that the GDPR could have been relied upon in taking action against Workplace, the Pensions Regulator's use of the Act led to custodial sentences for Workplace's directors. This serves as a clear sign to companies and their directors that, in addition to potential fines under the GDPR, the misuse of data can lead to custodial sentences.

The Pensions Regulator's actions may signal the start of a new approach with regulators using additional legal tools to combat the misuse of data rather than simply taking action under the GDPR. Whilst the Act and GDPR overlap in some respects, they apply in slightly different circumstances, thereby providing regulators with options depending on the facts of a case. In particular, the Act applies to unauthorised acts relating to computer systems regardless of whether personal data has been accessed. As mentioned above, the GDPR only applies to the misuse of personal data. In addition, the CMA only applies to specified acts relating to computer systems whereas the GDPR applies more broadly.

Workplace is likely to be particularly concerning to multinational technology companies that have been found in the past to have, for example, obtained data through the use of cookies and other technologies without first obtaining consent from users. Whilst fines under the GDPR may be seen as an unwanted cost or financial penalty, the potential application of criminal sanctions may cause companies to give second thought to making use of technologies in harvesting data without consent.