McCann FitzGerald

Ireland Finally Moves to Enact Dedicated Cybercrime Legislation

BRIEFING

Cybercrime is a major concern for Irish business and dedicated legislation to tackle this issue has been on the Government's agenda for some time. As early as 2008, Deputy Willie O'Dea outlined to the Dáil the Government's plans to implement the Criminal Justice (Cybercrime) Bill, that was then in preparation in the Department of Justice.

The purpose of this legislation was to enable the ratification of the Council of Europe Convention on Cybercrime[1] which Ireland had signed in 2002 and to transpose the 2005 EU Framework Decision on Attacks against Information Systems[2] which EU Member States were to have implemented by 16 March 2007.

However, this piece of legislation continued to languish on the outer reaches of the Government's legislative programme for a number of years until finally making the "A List" in Autumn 2015, retitled as the Criminal Justice (Offences relating to Information Systems) Bill. This Bill was finally published on 19 January 2016. The restated purpose of the Bill is to give effect to certain provisions of the EU Cybercrime Directive.[3] That Directive seeks to address the increasing occurrence of hacking and other attacks on computer systems, networks and data by improving co-operation between EU Member States and harmonising the law in respect of cybercrime. The Directive, which replaces the 2005 Framework Decision, was due for implementation by 4 September 2015. That date has now passed and unfortunately this first piece of Irish legislation to directly tackle cybercrime has fallen away as a result of the dissolution of the Dáil pending the upcoming general election. However, given the pressing need for action by Ireland here, it can be expected that when the new Dáil convenes that the Bill will be restored irrespective of the identity of the parties making up the next Government.

1 Council of Europe Convention on Cybercrime, Budapest 23.11.2001, CETS n° 185.

2 Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems.

3 Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems.

Ireland Finally Moves to Enact Dedicated Cybercrime Legislation

(continued)

The new legislation will also give Ireland scope to finally ratify the Cybercrime Convention as certain pieces of requisite domestic legislation will then be in place. The European Commission has, for some years, actively encouraged the ratification by Member States of the Convention given the importance of the instrument in the fight against cybercrime.

If enacted in its current form, the Bill would introduce five dedicated cybercrime offences:

- Accessing an information system[4] without lawful authority;
- Interfering with an information system without lawful authority so as to intentionally hinder or interrupt its functioning;
- Interfering with data without lawful authority;
- Intercepting the transmission of data without lawful authority; and
- Use of a computer, password, code or data for the purpose of the commission of any of the above offences.

The offence of interfering with an information system without lawful authority carries a maximum sentence on indictment of up to 10 years and the other offences carry maximum sentences of up to 5 years on indictment. The Court can treat identity theft as an aggravating factor when sentencing in respect of the offences of interfering with information systems and data. It will also be an offence to obstruct a Garda acting under the authority of a search warrant investigating a cybercrime offence,[5] and company officers may be liable individually if an offence was committed by the company with their consent or connivance.

This draft legislation is to be welcomed. Previous experience in Ireland and abroad has shown that attacks against information systems do require technology-specific legislation and cannot be satisfactorily regulated through the application of more general law provisions, as was attempted in the Criminal Damage Act 1991 where a decision was made to bring crimes involving computers within its scope rather than draft dedicated legislation. This was criticised at the time but the legislation went ahead. Certain deficiencies in the 1991 Act will also be addressed by the Bill, if it proceeds to enactment.

4 An "information system" means a device or group of devices one or more of which performs automatic processing of data pursuant to a programme; and data stored, processed, retrieved or transmitted by such a device for the purposes of the operation, use, protection or maintenance of the device or group of devices.

5 Section 7. This offence is punishable on indictment by up to 12 months imprisonment or a €5,000 fine.

McCann FitzGerald

Further information is available from:

Adam Finlay
Partner, Technology & Innovation

DDI +353-1-607 1795
EMAIL adam.finlay@mccannfitzgerald.ie

Karyn Harty
Partner, Dispute Resolution & Litigation

DDI +353-1-607 1220
EMAIL karyn.harty@mccannfitzgerald.ie

Béibhinn Bollard
Associate, Dispute Resolution & Litigation

DDI +353-1-607 1261
EMAIL bebhinn.bollard@mccannfitzgerald.ie

Alternatively, your usual contact in McCann FitzGerald will be happy to help you further.

Principal Office Riverside One, Sir John Rogerson's Quay, Dublin 2, D02 X576
Tel: +353-1-829 0000

London Tower 42, Level 38C, 25 Old Broad Street, London EC2N 1HQ
Tel: +44-20-7621 1000

New York Tower 45, 120 West 45th Street, 19th Floor, New York, NY 10036
Tel: +1-917-921 5077

Brussels 40 Square de Meeûs, 1000 Brussels
Tel: +32-2-740 0370

Email inquiries@mccannfitzgerald.com **www.mccannfitzgerald.com**