Harmful Communications and Digital Safety

This Report LRC 116-2016 Report on Harmful Communications and Digital Safety following on from the Commission's 2014 issues paper LRC IP 6-2014 Issues Paper on cyber-crime affecting personal safety, privacy and reputation including cyber-bullying and forming part of the Commission's Fourth Programme of Law Reform, contains 32 recommendations for reform. The Report also includes a draft Harmful Communications and Digital Safety Bill intended to implement these reforms.

The Report contains recommendations to reform both the criminal law (which already addresses some, but not all, harmful communications), as well a new statutory national oversight system that would promote and support positive digital safety.

Proposed criminal law reforms

The Report recommends the enactment of 2 new criminal offences to deal with posting online of intimate images without consent. The first is to deal with the intentional victim-shaming behaviour of posting intimate images without consent, often done after a relationship has broken down (so-called "revenge porn"). The second new offence also deals with posting intimate photos or videos and is to deal with a new type of voyeurism, often called "upskirting" or "down-blousing".

The Report also recommends reforms of the existing offence of harassment, to ensure that it includes online activity such as posting fake social media profiles; and that there should be a separate offence of stalking, which is really an aggravated form of harassment.

The Report also recommends reform of the existing offence of sending threatening and intimidating messages, again to ensure that it fully captures the most serious types of online intimidation.

A new statutory oversight system: a Digital Safety Commissioner to promote digital safety and oversee efficient take-down procedure

The Report also recommends that there is a need to establish a statutory Digital Safety Commissioner, modelled on comparable offices in Australia and New Zealand. The Commissioner's general function would be to promote digital safety, including an important educational role to promote positive digital citizenship among children and young people, in conjunction with the Ombudsman for Children and all the education partners.

The Report recommends that the Digital Safety Commissioner's role would also include publication of a statutory Code of Practice on Digital Safety. This would build on the current non-statutory take down procedures and standards already developed by the online and digital sector, including social media sites. The Code would set out nationally agreed standards on the details of an efficient take-down procedure.

Under the proposed statutory system, individuals would initially apply directly to a social media site to have harmful material removed in accordance with agreed time-lines: this is similar to the statutory system in place in Australia. If a social media site did not comply with the standards in the Code of Practice, the individual could then appeal to the Digital Safety Commissioner, who could direct a social media site to comply with the standards in the Code. If a social media site did not comply with the Digital Safety Commissioner's direction, the Commissioner could apply to the Circuit Court for a court order requiring compliance.

Other detailed recommendations

Among the other detailed recommendations in the Report are these:

- in any prosecution for a harmful communications offence provided for in the Report, the privacy of the person in respect of whom the offence is alleged to have been committed should be protected (but the victim should also be able to waive his or her anonymity);
- no prosecution for the offences discussed in the Report should be brought against children under the age of 17 except by or with the consent of the Director of Public Prosecutions: this reflects the Commission's view that, in the case of children and young people, the criminal justice process should be seen as a last resort and only after other responses, such as education or suitable diversion programmes, have been applied;
- the intent-based offences in the Report should carry, on summary conviction, maximum penalties of a Class A fine (currently, a fine not exceeding €5,000) and/or up to 12 months imprisonment; and on conviction on indictment, an unlimited fine and/or up to 7 years imprisonment
- a court should have the power to issue a restraining order restricting a person from communicating and/or approaching the victim of harmful communications, even if there has not been a criminal prosecution (currently, a restraining order can only be issued if a prosecution has been brought);
- the criminal offences and the civil law oversight of the proposed Digital Safety Commissioner should apply not only where the harmful communications occur in Ireland but also, where this is feasible, in relation to activity occurring outside the State (this is called extra-territoriality).