LAW REFORM COMMISSION

Opinion Paper

« Law on Social Media (Fake Profiles, Fake News and other Harmful Digital Communications) »

[LRC_R&P 126, September 2018]

13th Floor, SICOM Building II

Reverend Jean Lebrun Street

Port Louis, Republic of Mauritius

Tel: (230) 212-3816/212-4102

Fax: (230) 212-2132

E-Mail: lrc@govmu.org

URL http://lrc.govmu.org

About the Commission

THE LAW REFORM COMMISSION OF MAURITIUS consists of –

(a) a Chairperson, appointed by the Attorney-General;
(b) a representative of the Judiciary appointed by the Chief Justice;
(c) the Solicitor-General or his representative;
(d) the Director of Public Prosecutions or his representative;
(e) a barrister, appointed by the Attorney-General after consultation with the Mauritius Bar Council;
(f) an attorney, appointed by the Attorney-General after consultation with the Mauritius Law Society;
(g) a notary, appointed by the Attorney-General after consultation with the Chambre des Notaires;
(h) a full-time member of the Department of Law of the University of Mauritius, appointed by the Attorney-General after consultation with the Vice-Chancellor of the University of Mauritius; and
(i) two members of the civil society, appointed by the Attorney-General.

Under the direction of the Chairperson, the Chief Executive Officer is responsible for all research to be done by the Commission in the discharge of its functions, for the drafting of all reports to be made by the Commission and, generally, for the day-to-day supervision of the staff and work of the Commission.

The Secretary to the Commission is responsible for taking the minutes of all the proceedings of the Commission and is also responsible, under the supervision of the Chief Executive Officer, for the administration of the Commission.

The Commission may appoint staff on such terms and conditions as it may determine and it may resort to the services of persons with suitable qualifications and experience as consultants to the Commission.

LAW REFORM COMMISSION

Chairperson	: Mr. Gunness RAMDEWAR, OSK, SA [Attorney]
Chief Executive Officer	: Mr. Pierre Rosario DOMINGUE [Barrister]
Members	: Representative of Judiciary [Mr. Patrick Michel Tat KON KAM SING]
	Solicitor-General or his Representative [Mr. Dinay REETOO]
	Director of Public Prosecutions or his Representative [Mr. Satyajit BOOLELL, SC]
	Mrs. Narghis BUNDHUN, SC [Barrister]
	Mr. Gilbert NOEL [Attorney]
	Mrs. Wenda SAWMYNADEN [Notary]
	Mr. Hambyrajen NARSINGHEN [Law Academic (UoM)]
	Mr. Bernard MARIE [Member of Civil society]
Secretary	: Mrs. Saroj BUNDHUN

Staff & Human Resources

Chief Executive Officer : Mr. Pierre Rosario DOMINGUE

Law Reform Cadre

Senior Law Reform Officer : Mr. Sabir M. KADEL

Law Reform Officer : Dr. Goran GEORGIJEVIC

Law Reform Interns

Service to Mauritius (STM) : Ms. Tusha Luxmi JHUGEROO
: Mr. Heekesh RAMSURUN

Administrative Support Staff

Secretary : Mrs. Saroj BUNDHUN

Office Superintendent : Mrs. Marie Roselilette SOOBRAMANIA

Office Management Assistant : Mrs. Neelamani BANSRAM
: Mrs. Kajal RAMDUT

Senior Office Attendant/Technical Assistant : Mr. Subhas CHUMMUN

Driver/Office Attendant : Mr. Claude François JEAN-PIERRE
: Mr. Naraindranathsingh JANKEE

Executive Summary

Opinion Paper about "Law on Social Media (Fake Profiles, Fake News and other Harmful Digital Communications)" [LRC_R&P 126, September 2018]

The Law Reform Commission has undertaken, at the request of the Office of the Attorney-General, a comparative study of the law on fake profiles, fake news, and other harmful practices on social media.

The Commission has thus examined the current framework in our law, laws and practices in other jurisdictions [on matters, such as fake social media profiles and impersonation, fake news and misinformation, online harassment, stalking, grooming and sharing of intimate images].

In the light thereof, the Commission is recommending changes for reform of our law.

INTRODUCTION

1. Social networks are powerful and essential communication tools for individuals as well as for companies. Despite this, investing in social networks means each of us should have a perfect understanding of the legal issues and questions that regulate the Internet. Between fake news or hateful comments, it is often difficult to control the enormous mass of information that is created constantly on the Internet. Several countries have pondered into that question already and Mauritius cannot take the risk of being left behind.

2. For these reasons, the Law Reform Commission has embarked, at the request of the Attorney-General, on a review from a comparative perspective of laws in the UK, Germany, France, the USA, Australia, New Zealand, and Malaysia, relating to "fake news" (I), "fake profiles" (II), and "other harmful digital communications" such as online harassment, online incitement, stalking, threats and offensive messages, grooming, sharing of intimate images and hate speech (III) on social media and other electronic platforms (A), and studied the current legal framework in Mauritius and compared it to what have been done in other jurisdictions (B) in relation to digital safety. Finally, the Commission has examined options for changes in laws of Mauritius while balancing the increase need to digital safety with safeguarding the fundamental right to freedom of expression (C).

(A) COMPARATIVE LEGAL STUDY

FAKE NEWS

3. In January 2018, the European Commission set up a high-level group of experts (HLEG)[1] to advise on policy initiatives to counter fake news and disinformation spread online. The major recommendations as provided by the HLEG Report are as follows:
    - Enhance transparency of the online digital ecosystem.
    - Promote and sharpen the use of media and information literacy approaches to counter disinformation and help users navigate our media environment.
    - Develop tools for empowering users and journalists and foster a positive engagement with fast evolving information technologies.
    - Safeguard the diversity and sustainability of the European news media ecosystem.
    - Calibrate the effectiveness of the responses through continuous research on the impact of disinformation in Europe and an engagement process that includes predefined and time-framed steps combined with monitoring and reporting requirements.

[1] The HLEG was chaired by Professor DR. Madeleine de Cook Buning and consisted of 39 members who were tasked to advise the Commission on all issues arising in the context of false information spread across traditional and social media and on possible ways to cope with its social and political consequences.

FRANCE

4. In France, **the Senate Law Commission rejected on July 17, 2018 two bills[2] intended to combat false news** during the election period.[3] These two bills - ordinary[4] for the first, applicable during the European, legislative, senatorial elections and the referendums, organic[5] for the second, dedicated to the presidential election - aimed to allow a candidate or party to seize the "*juge des référés*" to **stop the dissemination of "false information" during the three months preceding a national election**. The first was adopted by 52 votes against 22, the second by 54 against 21, supported by LREM and a majority of MoDem. Moreover, they imposed on digital platforms like Facebook and Twitter obligations of transparency when they broadcast content for remuneration.

MALAYSIA

5. Earlier this year, Malaysia's parliament on Monday voted in favour of the world's first anti-fake news law.[6] The legislation provides for a fine of up to $123,000 and six-year jail sentences for anyone publishing or disseminating misleading information. It makes online service providers liable for third party content. And it has extraterritorial reach as fake news generated outside the country is subject to criminal penalties if either the country of Malaysia or Malaysian citizens are affected. Law Minister Azalina Othman Said told parliament: "This law aims to protect the public from the spread of fake news, while allowing freedom of speech as provided for under the constitution".[7]

---

[2] http://www.assemblee-nationale.fr/15/propositions/pion1219.asp
[3] https://francais.rt.com/france/52558-senat-propositions-loi-contre-fausses-nouvelles-rejetees-commission
[4] The ordinary laws intervene in the areas of the law defined in article 34 of the Constitution.
[5] The organic laws (Article 46 of the Constitution) are generally intended to specify the organization and functioning of public authorities in application of articles of the Constitution. The Constitutional Council has developed a jurisprudence which seeks in particular that the organic laws intervene only in the fields and for the objects limitatively enumerated by the Constitution.
[6] https://www.cljlaw.com/files/bills/pdf/2018/MY_FS_BIL_2018_06.pdf
[7] https://www.reuters.com/article/us-malaysia-election-fakenews/malaysia-outlaws-fake-news-sets-jail-of-up-to-six-years-idUSKCN1H90Y9

6. **Subsection 4(1) of the Act makes it an offence to "knowingly create, offer, publish, print, distribute, circulate or disseminate fake news"**. Subsection 4(3) also provides eight examples to clarify what it defines as fake news. Subsection 4(3)(a) states: "A offers false information to B, for B to publish the information in B's blog. B, not knowing that the information provided by A is false, publishes the information in his blog. A is guilty of an offence under this section. B is not guilty of an offence under this section". **Subsection 3(1) deals with extraterritoriality and determines the legislation applies not only to Malaysian citizens but to "any person, whatever his nationality or citizenship"**. Meanwhile, subsection 3(2) determines the Act finds application if the "fake news" concerns Malaysia, or "the person affected by the commission of the offence is a Malaysian citizen". Anyone found in contravention of the legislation can be fined up to $123,000 or sentenced to up to ten years' imprisonment. Subsection 4(2) of the Act also determines that a person convicted of the aforementioned offences can be compelled by the Court to "apologise" to those affected. Persons who refuse to remove "fake news" from a publication were also liable to pay a fine of up to $25,000.

   This law attracted a lot of criticisms. Thus, "Malaysia's 'fake news' bill is a blatant attempt by the government to prevent any and all news that it doesn't like, whether about corruption or elections," alleged Brad Adams, Asia director of NGO, Human Rights Watch. "The proposed law uses draconian penalties and broad language in an audacious and unprecedented effort to control discussion of Malaysia worldwide."[8]

   In a letter sent by an Ambassador of Malaysia, Dato' Amran Mohammed Zin, to the UN's Special Rapporteur on freedom of opinion and expression, David Kaye, on 11th June 2018, it was announced that the anti-fake news would be repealed.[9] On August 16th

[8] https://www.hrw.org/news/2018/03/29/malaysia-drop-proposed-fake-news-law
[9] https://www.ohchr.org/Documents/Issues/Opinion/Legislation/ReplyMalaysiaOL.pdf

this year, it was officially revoked.[10] According to Deputy Minister in the Prime Minister's Department, Mohamed Hanipa Maidin, in his winding-up speech, there were sufficient laws to deal with fake news and said "We don't need new legislations. We already have existing laws, such as the Communications and Multimedia Act 1998 and others that can deal with this phenomenon".[11]

Yale Law School Fighting Fake News Workshop Report

7. On March 7, 2017, the Information Society Project at Yale Law School and the Floyd Abrams Institute for Freedom of Expression held a workshop[12] with the intention to explore the ongoing efforts to define fake news and discuss the viability and desirability of possible solutions.

8. Participants in the workshop determined that the most salient danger associated with "fake news" is the fact that it devalues and delegitimizes voices of expertise, authoritative institutions, and the concept of objective data—all of which undermines society's ability to engage in rational discourse based upon shared facts. It was also noted that while there is a general awareness of the existence of "fake news," there is widespread disagreement over what comprises "fake news." Merely labeling something as "fake news" can itself be considered mere propaganda, making it all the more important that journalists cite sources and "show their work."

9. It was also considered how misinformation spreads and the role of online social media in creating and exacerbating echo chambers and filter bubbles. It was moreover said that one benefit to governmental regulation is that it can address problems that platforms

[10] https://www.malaymail.com/s/1663132/anti-fake-news-bill-repealed-despite-fierce-resistance
[11] https://www.thestar.com.my/news/nation/2018/08/16/parliament-passes-bill-to-repeal-anti-fake-news-law/
[12] https://law.yale.edu/system/files/area/center/isp/documents/fighting_fake_news_-_workshop_report.pdf

would like to address but feel unable to do so, either because they do not wish to be tarred as censors or because the economic incentives run contrary to their interfering with user access to content unless their competitors do so as well. Another potential benefit to increased intermediary liability would be that it might encourage content intermediaries to view themselves as the media companies of the 21st century, with all of the normative obligations that entails.

10. Nearly all participants agreed on one overarching conclusion: that reestablishing trust in the basic institutions of a democratic society is critical to combat the systematic efforts being made to devalue truth. It was suggested that Content consumers must be better educated, so that they are better able to distinguish credible sources and stories from their counterparts. It was also asserted that Content distributors, particularly digital content distributors, should engage in practices that minimize the spread of fake news and promote the dissemination of trustworthy, high-quality information.

11. Finally, it was said that there may be relatively few legal tools capable of addressing aspects of the "fake news" problem, but the few that exist can be used to neutralize some of the worst, most manifestly false and profit-driven pieces. Platform terms of service (such as rules against impersonation and abuse) can be better enforced, either by the platforms taking the initiative to do so themselves or by permitting third-party enforcement of terms of service.

FAKE PROFILES

12. Most social media sites cover policies on posting private information such as addresses and bank details and policies on impersonation, which proscribe users from setting up fake profiles to mislead or confuse other users.

13. Perpetrators can be unknown or adopt multiple online personae and build fake profiles as a platform to attack others. The capability to send anonymous texts and comment anonymously may have a disinhibiting effect on the communicator, detaching them from their victim and the consequences of their actions; while from the victim's perception, the anonymity of the abuser can exacerbate the victim's sense of powerlessness.[13]

IRELAND

14. One way of conceptually understanding fake profiles is through **indirect harassment**. Indirect online harassment comprises persistent harmful communications through email, social media sites or other digital or online means to third parties concerning a person but not openly communicated to the person. It would include, for instance, circumstances where a defendant disseminates harmful information shall they be true or false to the person's friends or family. It might also involve repeatedly posting content online to the public at large concerning a person.

15. In the **Ireland Law Reform Commission's 2013 Report on Aspects of Domestic Violence,**[14] it was recommended that indirect harassment should be an offence. Section

[13] New Zealand Law Commission, Ministerial Briefing Paper on "Harmful Digital Communications: the adequacy of the current sanctions and remedies", August 2012, para. 2.42
[14] http://www.lawreform.ie/_fileupload/reports/r111.pdf

10 of the Irish Non-Fatal Offences Against the Person Act 1997 requires that the accused engage in "following, watching, pestering, besetting or communicating with" the victim. The requirement to communicate with the victim means that it is unlikely that section 10 could be interpreted as applying to all forms of indirect activity. So where the offending communication is sent not to the victim but to others there may be no communication with the victim. Similarly, harmful messages posted on a private social media page such as on Facebook may also not be covered by section 10 if they do not involve direct communication with the subject.

In its **Report on "Harmful Communications and Digital Safety"**,[15] the Ireland Law Reform Commission recommended that **section 10 of the Non-Fatal Offences Against the Person Act 1997 should be repealed, and replaced by an offence of harassment** that is modelled on section 10 and that includes two additional provisions: **(a) that the harassment offence should expressly apply to harassment by any means of communication, including through digital and online communications; and (b) that it should deal with indirect form of communications, such as setting up fake online social media profiles.**[16]

16. Providing for indirect harassment would not constitute a drastic change to the harassment offence because the direct link between the perpetrator and the victim would be retained. This is because while the indirect behaviour may appear to be directed at a third party, **the behaviour would still need to be such that it can be proven that it harasses the victim**. The behaviour must thus really impede on the victim's peace and privacy or cause him or her alarm, distress or harm as well as satisfy the requirement that a

[15]http://www.lawreform.ie/_fileupload/Final%20Report%20on%20Harmful%20Communications%20and%20Digital%20Safety%2021%20Sept%20PM.pdf
[16] Para. 2.54 of the Report on "Harmful Communications and Digital Safety".

reasonable person would realise that the harassing acts would seriously interfere with the victim's peace and privacy or cause the victim alarm, distress or harm. **These elements of the proposed amended harassment offence would prevent prosecutions for behaviour such as gossiping or the sharing of lawful content.**

USA

17. The Congress in the United States enacted the **Federal Identity Theft and Assumption Deterrence Act (1998)**[17] in order to criminalise the act of impersonation. According to Section 18 U.S.C paragraph 1028 (a) of the enactment, any person who knowingly possess or use, without lawful authority, a means of identification of another person with the intent to commit any unlawful activity that constitutes a violation of Federal highlighted law or any applicable State or local law shall commit a federal crime.

18. The State of New York enacted an amendment to the Penal Law making it a crime to impersonate another person or pretend to be a public servant by means of online communications.[18] More specifically, New York's Internet impersonation law amends section 190.25 of the Penal Law by adding sub division 4, **making it a crime to impersonate another person by electronic means, including the use of a website, with the internet to obtain a benefit or injure or defraud another person**. The amendment states that the internet impersonation offence is a class A misdemeanour and carries a maximum penalty of a $1,000 fine and a one-year term of imprisonment for each violation and each act of impersonation.

[17] https://www.ftc.gov/node/119459
[18] https://codes.findlaw.com/ny/penal-law/pen-sect-190-25.html

OTHER HARMFUL DIGITAL COMMUNICATIONS

19. Harmful digital communications can take many contours. First, they can be in the form of direct harassment, which relates to threatening or harassing messages sent to the victim. It consists often of repeated attempts to target specific persons by directly contacting them. Direct harassment (i) must be distinguished from indirect harassment, which does not target directly the victim but which has collateral effects which can cause distress to someone, like in the case of fake profiles, as we have seen above.

20. There is then stalking (ii), which is a form of harassment, but where the offender has a more personal relationship to the victim than in classical modes of harassment. Moreover, some harmful digital communication can be only "once-off" (iii), the content being uploaded only once, and which would not thus fall under classic harassment offences which consist of repeated conducts.

21. Threats, Intimidation and Offensive Messages (iv) are another kind of harmful digital communications which are common on social media platforms and which are made even more easy and dangerous by the feeling of anonymity which the authors of those acts enjoy. Sometimes, ill-intentioned people also incite others to commit acts which might endanger their life (v), which is another issue which the law must address to make the internet a safer place for everyone, mainly for minors.

22. Another criminal behavior which sometimes takes place over the internet is what is dubbed as grooming (vi) which is the process used by adults with a sexual interest in children to prepare a child for sexual abuse. It is often very carefully calculated and it can take place over weeks, months or even years.

23. Just like in real life, some people over the internet are assaulted by messages which can be deemed obscene or indecent (vii). Moreover, with the advent of social media, another practice has developed and which is frequently known in the media as "revenge porn" where someone's intimate images are distributed without his consent (viii).

24. Finally, the Internet with its unique facility of communication of one-to-many and many-to-many and its potential for anonymous and mobile interaction has become the new platform for the diffusion of hate speech. To deal with this issue, countries have been tempted to enact legislation criminalizing online hate speech (ix).

(i) Direct harassment

25. Harassment by means of digital or online communication is as harmful as offline harassment and possibly, it can even be more damaging because of the specific features of digital communications. Digital communications have the ability to be instant, numerous, reach large even global audiences, be enduringly available and are often anonymous in nature. Harassment by digital or online means can also have an inescapable quality as the victim can be targeted anytime and anywhere because of the ubiquity of portable internet connected devices such as smartphones. Thus, the potential for harassment by digital or online means to cause substantial harm is significant and it has been linked to serious psychological harm and even in extreme cases to suicide. When it is directed specifically towards children, it is often characterised as online bullying.

IRELAND

26. The Ireland Law Reform Commission, in its Report on "Harmful Communications and Digital Safety", **considered amending the harassment offence to include a specific reference to harassment by digital or online means**. This would offer important clarification as to the scope of the offence, similar to the specific mention of harassment by telephone which is already included in section 10 of the Non-Fatal Offences Against the Person Act 1997.[19] This clarification could lead to an increase in reporting of this type of harassment. Expressly identifying harassment by digital or online means in the legislation as a particular form of the wider offence of harassment would also underline society's recognition of its seriousness and the need to prevent and punish it. However, **educational measures aimed at the general public** and the Gardaí, according to the Commission, are also necessary to increase public awareness of the capacity of the harassment offence to be used in cases involving harassment by digital or online means and to offer guidance to the Gardaí as to when the offence is applicable.[20]

    The reference in section 10 to "telephone" without any mention of other forms of electronic communication makes the section appear outdated. Thus, including a reference to harassment by digital or online communication **would clarify and modernise the wording of the harassment offence**. It would also correctly label the conduct that is covered by the offence and ensure that harassment by digital or online means is not a hidden form of harassment as section 10 of the 1997 Act currently suggests.[21]

27. The Commission thus recommends that section 10 of the Non-Fatal Offences Against the Person Act 1997 be repealed and replaced with a harassment offence which expressly applies to harassment by all forms of communication including through digital and online

[19] http://revisedacts.lawreform.ie/eli/1997/act/26/section/10/revised/en/html
[20] Para. 2.29 of the Report on "Harmful Communications and Digital Safety".
[21] Para. 2.30 of the Report on "Harmful Communications and Digital Safety".

communications such as through a social media site or other internet medium. The Commission recommends that **this amendment be made by including a definition of "communication" in the legislation which would extend to any form of communication including by letter, telephone (including SMS text message) or digital or online communication such as through a social media site or other internet medium**. The Commission has also concluded that the existing criminal law on harmful communications, together with the reforms proposed in this Report, should be consolidated into a single piece of legislation.[22]

AUSTRALIA

28. In Australia, in March 2015, the **Enhancing Online Safety for Children Act 2015** became law.[23] This Act provides for a new civil enforcement mechanism designed to ensure the swift removal of harmful online content. However, it only applies to cyber-bullying involving children. The Act introduces a Children's e-safety Commissioner whose main function is to administer a complaint system in relation to cyber-bullying material which targets Australian children.[24] **"Cyber-bullying material" is defined as material provided on a social media service or other electronic service which an ordinary reasonable person would conclude was intended to have the effect of "seriously threatening, seriously intimidating, seriously harassing or seriously humiliating" a child**. The Commissioner also has additional functions including the promotion of online safety for children and coordinating the activities of other authorities and agencies in the area of internet safety.

[22] Para 2.31 of the Report on "Harmful Communications and Digital Safety".
[23] https://www.ilo.org/dyn/natlex/docs/ELECTRONIC/105254/128682/F-237304532/AUS105254.pdf
[24] Section 15 of the Enhancing Online Safety for Children Act 2015.

29. **This Act has been met with some criticism** from commentators such as Berg and Breheny, who view it as "**a serious threat to freedom of speech and digital liberties**" and **an intrusion into the realm of civil society and the relationships between parents and children.**[25] They argue that granting the Commissioner the power to **issue notices to children requiring them to apologise** is an intolerable interference by the government into the domain of parents and schools. They suggest that one of the great challenges in developing policies to tackle bullying is that the "dynamics of social relationships among children are extremely opaque to outsiders" and the relationships between children are highly fluid. Thus, behaviour which may appear to adults to be threatening, may not be understood as such by children. Inserting the state in the form of a body like the e-safety Commissioner is therefore highly undesirable as it has the potential to stifle children's freedom of speech and act as a form of censorship. It may also **drive cyber-bullying underground away from mainstream sites** such as Twitter and Facebook and onto less controlled sites.

(ii) Specific Stalking Offence

30. Even though stalking is frequently described as a form of harassment there is an argument that it is a distinct crime deserving of specific recognition. Indeed, "Somebody might harass another person because they are not happy with them or whatever, but that is slightly different from the intimate relationship that stalker has with his victim. There is an emotional relationship between two people, and it is an unequal relationship."[26]

[25] Berg and Breheny (Institute of Public Affairs) A social problem not a technological problem: Bullying, cyber-bullying and public policy (August 2014) at 3.
[26] Independent Parliamentary Inquiry into Stalking Law Reform, Main Findings and Recommendations (Justice Unions' Parliamentary Group, 2012) at 11.

SCOTLAND

31. In Scotland, section 39 of the **Criminal Justice and Licensing Scotland Act 2010**[27] provides for an offence of stalking. This offence is **committed when a person stalks another person by engaging in a course of conduct with the intention of causing fear or alarm, or when he or she knows or ought to have known that engaging in the course of conduct would cause the victim fear or alarm, and the course of conduct causes the victim to suffer fear or alarm.**[28] Defences are included for lawful behaviour, behaviour engaged in for the purpose of preventing or detecting crime or where the course of conduct was reasonable in the circumstances.[29]

ENGLAND AND WALES

32. In 2012, England and Wales introduced the **Protection of Freedoms Act 2012**[30] which **inserted two new stalking offences into the Protection from Harassment Act 1997.** These offences were introduced because the Protection from Harassment Act 1997 was regarded as being unsuccessful at targeting stalking. The main problem identified with the Protection from Harassment Act 1997 was its breadth,[31] in particular, it "did not go far enough to identify and prosecute the types of behaviour that distinguish stalking from other, milder cases of harassment".[32] Thus, the 1997 Act was described as "no longer fit for purpose"[33] as cases of stalking and harassment continued to increase since the 1997

[27] https://www.legislation.gov.uk/asp/2010/13/contents
[28] Section 39(1), (2) of the Criminal Justice and Licensing (Scotland) Act 2010.
[29] Section 39(5) of the Criminal Justice and Licensing (Scotland) Act 2010.
[30] http://www.legislation.gov.uk/ukpga/2012/9/contents/enacted
[31] Independent Parliamentary Inquiry into Stalking Law Reform, Main Findings and Recommendations (Justice Unions' Parliamentary Group, 2012) at 21.
[32] House of Lords Debate on Protection of Freedoms Act 2012 (6 December 2011), col. 650 available at http://www.publications.parliament.uk/pa/ld201011/ldhansrd/text/111206-0001.htm#11120644000422
[33] Independent Parliamentary Inquiry into Stalking Law Reform, Main Findings and Recommendations (Justice Unions' Parliamentary Group, 2012) at 21.

Act was passed, and dissatisfaction was expressed by stalking victims who felt that their cases had not been taken seriously by the criminal justice system.

33. The Protection of Freedoms Act 2012 inserted sections 2A (offence of stalking)[34] and 4A[35] (stalking involving fear of violence or serious alarm or distress) into the Protection from Harassment Act 1997. **Under section 2A, a person is guilty of an offence if they pursue a course of conduct that amounts to stalking.**[36] A person pursues a course of conduct amounting to stalking if the course of conduct amounts to harassment, the acts or omissions involved are associated with stalking and the person knows or ought to have known that the course of conduct amounts to harassment.[37] The section then enumerates "examples of acts or omissions which, in particular circumstances, are ones associated with stalking".[38]

IRELAND

34. In Northern Ireland, stalking cases are currently prosecuted under the harassment offences in sections 4 and 6 of the **Protection from Harassment (Northern Ireland) Order 1997**[39] (which roughly correspond to the harassment offences in the English and Welsh Protection from Harassment Act 1997).

35. The Ireland Law Reform Commission, in its Report on "Harmful Communications and Digital Safety" suggested **that a stalking offence, separate from the related offence of**

[34] https://www.legislation.gov.uk/ukpga/1997/40/section/2A
[35] https://www.legislation.gov.uk/ukpga/1997/40/section/4A
[36] Section 2A(1)of the Protection from Harassment Act 1997.
[37] Section 2A(2) of the Protection from Harassment Act 1997.
[38] Section 2A(3) of the Protection from Harassment Act 1997.
[39] https://www.legislation.gov.uk/nisi/1997/1180/contents

harassment, should be introduced. The Commission considers that the essential ingredients of the stalking offence should be the same as the proposed, amended, harassment offence, so that the offence would be **committed where a person "stalks" another person by persistently following, watching, pestering or besetting another person or by persistently communicating by any means of communication with the other person or by persistently communicating with a third person by any means of communication about the other person.**[40] For the purposes of this offence, a person would stalk another person where he or she, by his or her acts intentionally or recklessly, seriously interferes with the other person's peace and privacy and causes alarm, distress or harm to the other person and his or her acts are such that a reasonable person would realise that the acts would seriously interfere with the other person's peace and privacy and cause alarm, distress or harm to the other person. Thus, the stalking offence would fluctuate from the harassment offence by **necessitating the intentional or reckless acts of the perpetrator to interfere seriously with the victim's peace and privacy** and cause him or her alarm, distress or harm, as opposed to the harassment offence which makes these alternative requirements. This additional threshold that would need to be met for the stalking offence to be committed, as opposed to harassment, **underlines stalking's status as an aggravated form of harassment**.

(iii) Offences Designed to Target Once-off Harmful Digital Communications

36. Limiting harassment to persistent behaviour implies that posting content online by a single upload which seriously interferes with a person's privacy will not amount to harassment because the communication will not have been made persistently. The internet and other digital communications technologies have created new and potentially

[40] Para. 2.73 of the Report on "Harmful Communications and Digital Safety".

treacherous ways in which individual privacy can be compromised. The online world leaves individuals defenceless to serious privacy violations through the posting of private, false, humiliating, shameful or otherwise harmful content, notably through social media sites such as Facebook, Twitter or YouTube, without the consent of the subject. The harm that is caused by such violations of privacy can be substantial because content that is posted online can be disseminated instantly and widely, possibly reaching global audiences.[41]

37. The permanence of online content as well as the potential for such content to go viral and remain in the public consciousness and publicly available after the initial upload means that such interferences with privacy can have substantial long-term consequences, such as harming future employment prospects and having harmful effects on the individual's physical or mental health. This is despite the fact that the content may only have been uploaded once.

NEW ZEALAND

38. In 2015, New Zealand introduced an offence of "causing harm by posting a digital communication" under **section 22 of the Harmful Digital Communications Act 2015**.[42] This offence is **designed to target harmful once-off digital communications**. This offence is committed where a person posts a digital communication with the intention to cause harm to a victim and this action would cause harm to a reasonable person in the

[41] O'Higgins Norman "Report on Cyberbullying Research and Related Issues" Conference Paper, 1st National Cyberbullying Conference (1 September 2014) at 3, where the author notes that "a single action, which is then shared or repeated by others, may be as harmful as repeated incidents".
[42] http://www.legislation.govt.nz/act/public/2015/0063/latest/whole.html#DLM5711856

position of the victim and the posting causes harm to the victim.[43] The Act defines "harm" as "serious emotional distress".[44]

39. This offence has been subjected to considerable criticism since the Harmful Digital Communications Act 2015 was passed. Critics argue that the offence is overbroad and vague, particularly the definition of harm and the factors which can be taken into account when assessing whether harm is caused.[45] It has also been suggested that the offence has created a situation whereby **behaviour which is legal offline is illegal online as the offence captures a very wide category of speech**. In this respect, one observer highlighted that public interest speech such as exposing corruption online could be covered by the offence as well as parody and satire. The offence has thus been described as a "threat to online free speech".

UK

40. In the UK, there are two offences susceptible of applying to once-off harmful online communications on a general basis: **section 1 of the Malicious Communications Act 1988 and section 127 of the Communications Act 2003.**[46] Section 1 of the Malicious Communications Act 1988 **provides for an offence of (a) sending a letter, electronic communication or article of any description which conveys a message which is indecent or grossly offensive, a threat or information which is false and known or believed to be false by the sender and (b) "sending an article or electronic communication which is, in whole or part of an indecent or grossly offensive**

[43] Section 22(1) of the Harmful Digital Communications Act 2015.
[44] Section 4 of the Harmful Digital Communications Act 2015.
[45] See, for example, "New law poorly-drafted, vague, and could criminalise free speech" Stuff.co.nz 6 July 2015 available at http://www.stuff.co.nz/the-press/opinion/69955436/new-law-poorlydrafted-vague-and-could-criminalise-free-speech.
[46] https://www.legislation.gov.uk/ukpga/1988/27/section/1

nature". The offence carries a maximum sentence of 12 months on summary conviction and 2 years for conviction on indictment. **Under section 127 of the Communications Act 2003, a person who sends, by a public electronic communications network, a message or other matter that is grossly offensive, indecent, obscene or menacing or causes such a message or other matter to be sent is guilty of an offence**. The section also makes it an offence to send or cause to be sent false messages by means of a public electronic communications network or to persistently make use of a public electronic communications network for the purpose of causing annoyance, inconvenience or needless anxiety. This is a summary offence and carries a maximum term of imprisonment of 6 months. A message sent by a "public electronic communications network" has been held to include a message sent by Twitter and to also extend to other communications sent via social media which are "accessible to all those who have access to the internet".

(iv) Threats, Intimidation and Offensive Messages

NEW ZEALAND

41. The New Zealand Law Commission considers, in its Paper on Harmful Digital Communications, that there should be an offence of sending an offensive message with intent to cause distress. The Commission proposed that the elements of the proposed offence should be:[47]

(a) The message must be grossly offensive, or of an indecent obscene or menacing character, or knowingly false.

(b) The sender must either:

[47] Para. 4.76 of the Paper on Harmful Digital Communications.

(i) Have an intention to cause substantial emotional distress or,

(ii) Know that the message will cause substantial emotional distress.

(c) The message must be such as would cause substantial emotional distress to a reasonable person in the position of the victim.

(d) The message need not be directed specifically at the victim, provided that it is placed in the electronic media and is in fact seen by the victim.

(e) In determining whether a message is grossly offensive, the court should take into account such factors as the extremity of the language employed; the age and characteristics of the victim; whether the message was anonymous; whether the message was repeated; the extent of the circulation of the message; whether the message is true or false (in some contexts truths are more hurtful than falsity, in others the reverse is the case); and the context in which the message appeared (different fora may lead users to expect different levels and styles of discourse).

(v) Incitement

NEW ZEALAND

42. The Law Commission of New Zealand considers in its above quoted Report, that there is **no need to create a specific offence of inciting offensive communication**, as it is caught by the more general provisions, mainly by Section 311 of the Crimes Act 1961 which provides that anyone who incites, counsels or attempts to procure any person to commit any offence, even if the offence is not committed, is liable to the same

punishment as if they had attempted to commit the offence. In other words, incitement to commit an offence is itself already an offence in New Zealand.[48]

43. Nevertheless, it is of the view that given the distress such incitements may cause in themselves, let alone the possibly devastating outcome, there is a strong argument for making incitement of suicide in itself criminal, like it is the case in Canada, where the Canadian Criminal Code criminalises counselling a person to commit suicide "whether suicide ensues or not".[49]

(vi) Grooming

NEW ZEALAND

44. The Law Commission of New Zealand is in favour of a provision **that makes the process of grooming criminal in itself, even though no overt act has been done in preparation for a meeting**. It proposes that it be an offence if a person:

(a) engages in any conduct that exposes a person under the age of 16 years (the young person) to indecent material; and

(b) does so with the intention of making it easier to procure the young person for unlawful sexual activity with him or her or any other person.[50]

[48] Para. 4.81 of the Report.
[49] Criminal Code of Canada RSC 1985 c C-46, s 241.
[50] Para. 4.88 of the report on Harmful Digital Communications.

(vii) Offence of distributing a threatening false, indecent or obscene message

IRELAND

45. The Law Reform Commission of Ireland recommends, that section 13 of the Post Office (Amendment) Act 1951 be repealed and replaced with a new offence designed to apply to all forms of communication including messages distributed online through social media, and that this **should include not only messages to a person but also about a person.** This new offence would be committed **where a person intentionally or recklessly for the purpose of causing alarm, distress or harm, by any means of communication distributes or publishes a threatening, false, indecent or obscene message to or about another person or distributes or publishes such a message persistently**. This is broadly based on the factors in section 13 of the 1951 Act, but the wording has been aligned with the "harm" test in section 10 of the Non-Fatal Offences Against the Person Act 1997. The new offence of distributing a threatening, false, indecent or obscene message reflects section 13 of the 1951 Act in that one act is sufficient for the offence to be committed. The offence also reflects section 13 of the 1951 Act by being capable of applying to persistent acts, and can thus be compared with the restated harassment offence and the new stalking offence. This new offence thus amends the wording of section 13 by **omitting the word "grossly offensive" and replacing "menacing" with "threatening" as these terms ("grossly offensive" and "menacing") could be vulnerable to constitutional challenge on grounds of vagueness**. The Commission considers that the other terms used in the offence are also sufficiently clear.[51]

[51] Para. 2.184.

(viii) Distribution of intimate images offences

46. The publication of intimate pictures without the consent of the subject is a form of privacy intrusion. The level of harm and distress that is caused is major.

NEW ZEALAND

47. The Law Commission of New Zealand is of the view that the reported level of online publication of intimate visual recordings now warrants an amendment to the Crimes Act to **criminalise the publication of intimate images by the person who made the image, without the consent of the person depicted**. Accordingly, it recommends that the covert filming provision of the Crimes Act 1961 be amended to provide that it is an offence for the creator of an intimate picture to publish it without consent **even though the picture may have been taken originally with subject's consent.**[52]

IRELAND

48. The Ireland Law Reform Commission proposes that an offence be introduced to target the distribution or publication, by any means, of an intimate image without the consent of the person depicted in the image. This offence should also extend to threats to publish or distribute an intimate image. This offence would be committed where by publishing or distributing the intimate image or threatening to do so, **the perpetrator intentionally or recklessly seriously interferes with that person's peace or privacy or causes alarm distress or harm to the person depicted in the image and a reasonable person would realise that the publication or distribution of the image would seriously interfere with the peace and privacy of the person depicted in the image or cause them alarm, distress or harm**. Thus, the essential ingredients of the offence would mirror those

[52] Para. 4.94 of the report on Harmful Digital Communications.

presently found in section 10 of the Non-Fatal Offences Against the Person Act 1997 except that this offence would not require persistence and could involve a once-off act.[53]

49. Moreover, the Ireland Law Reform Commission recommends that a separate offence be introduced to target the **non-consensual taking and distribution of intimate images, by any means of communication, without intent to cause alarm, distress or harm**. This offence is aimed at behaviour that falls short of the intentional, egregious, activity associated with the shaming offence sometimes referred to as "revenge porn" that would be dealt with through the offence involving the distribution of intimate images without consent or threatening to do so with the intent to cause harm. The offence of taking or distributing an intimate image without consent may, in some respects, be thought of as being associated with the behaviour known as "sexting" but it differs in a fundamental way in that it is **committed only where the intimate image is taken without consent.** It remains a separate question, which is outside the scope of the criminal law, as to whether it is appropriate or suitable for persons, whether young persons or adults, to distribute intimate images.[54]

50. The Commission recommends adopting a definition of "intimate image" based on the definition of "intimate image" inserted into the Canadian Criminal Code under the Protecting Canadians from Online Crime Act 2014. [55] This definition would **apply to visual recordings made by any means including a photographic, film or video recording in which the person depicted is nude, is exposing his or her genital organs or anal region or her breasts or is engaged in sexual activity**. However, the Commission proposes that images depicting a person's genital or anal region, or in the

[53] Para. 2.191.
[54] Para. 2.194.
[55] Section 162.1(2) of the Canadian Criminal Code.

case of a female, her breasts, where the genital or anal region or breasts are covered by underwear, should also be included in the definition of "intimate image" as this would ensure that **"upskirting" and "downblousing" images, which do not involve nudity, are covered.**

(ix) Hate Speech

51. In 2008, the EU adopted a Framework Decision on combating certain forms and expressions of racism and xenophobia by means of criminal law,[56] which contains very similar provisions to the Additional Protocol the Council of Europe Convention on Cybercrime.[57] Thus, the Framework Decision requires that Member States take necessary measures to ensure that the following intentional conduct is punishable:

(a) publicly inciting to violence or hatred directed against a group of persons or a member of such a group defined by reference to race, colour, religion, descent or national or ethnic origin;

(b) the commission of an act referred to in (a) by public dissemination or distribution of tracts, pictures or other material;

(c) publicly condoning, denying or grossly trivialising crimes of genocide, crimes against humanity and war crimes.

The Framework Decision also requires that Member States ensure that their legislation extends to cases where the conduct is committed through an information system and the offender is within the territory of the Member State, even if the content hosted is not, and

[56] Council Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law.
[57] https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081601

to cases where the material is hosted within the territory of the Member State whether or not the offender commits the conduct when physically present in its territory. In its 2014 report on the implementation of the Framework Decision, the EU Commission noted that **online hate speech is one of the most prevalent ways of manifesting racist and xenophobic attitudes and that Member States should have a means to intervene in such cases.**[58] The Framework Decision also provides that a Member State shall take necessary measures to establish jurisdiction where the conduct has been committed by one of its nationals.

GERMANY

52. In Germany, since October 2017 the Act to Improve Enforcement of the Law in Social Networks (NetzDG) regulates the fight against "fake news" and "hate crime" in social networks. The NetzDG shall **ensure that certain unlawful contents are removed or blocked after a complaint was lodged.** S1 (3) NetzDG defines unlawful content as content that fulfils the requirements of the offences described in SS86, 86a, 89a, 91, 100a, 111, 126, 129 to 129b, 130, 131, 140, 166, 184b in connection with 184d, 185 to 187, 201a, 241 or 269 of the Criminal Code and which is not justified. In essence, these are contents that violate norms which affect the protection of the democratic constitutional state, public order, personal honour and sexual self-determination.

53. As stipulated in S3 (2) No. 2 NetzDG, **manifestly unlawful contents shall be removed within 24 hours of receiving the complaint**, whereby a longer period of time for blocking or deletion can be agreed individually with the competent law enforcement authority. A manifestly unlawful content is given if the **unlawfulness can be detected**

[58] Report from the Commission to the European Parliament and the Council on the implementation of Council Framework Decision 2008/913/JHA on combating certain forms and expressions of racism and xenophobia by means of criminal law (January 2014) at 8.

without any in-depth examination, i. e. it can be examined immediately by trained personnel, but with reasonable effort and in any case within 24 hours.

54. According to S3 (2) No. 3 NetzDG, the access to other unlawful contents shall be removed or blocked without delay and generally within seven days. This time limit may be exceeded if the decision regarding the unlawfulness of the content is dependent on the falsity of a factual allegation or is clearly dependent on other factual circumstances. In such cases, the social network can **give the user an opportunity to respond to the complaint before the decision is rendered**. In addition, S3 (3) No. 3 lit. b) NetzDG allows the social network to refer the decision regarding unlawfulness to a recognised self-regulation institution within seven days of receiving the complaint and agrees to accept the decision of that institution. In the case of removal, the content shall be retained as evidence and stored for this purpose within the scope of Directives 2000/31/EC and 2010/13/EU for a period of ten weeks (S3 (2) No. 4 NetzDG). Besides, the person submitting the complaint and the user shall be notified immediately about any decision, while also be provided with reasons for the decision (S3 (2) No. 5 NetzDG).

55. In addition, the management of the social network shall **monitor the established procedure via monthly checks and offer training courses and support programs** delivered in the German language on a regular basis to the persons tasked with the processing of complaints (S3 (4) NetzDG). Moreover, providers of social networks which receive more than 100 complaints per calendar year about unlawful content shall be obliged to produce half-yearly German-language reports on the handling of complaints about unlawful content on their platforms and shall be obliged to publish these reports in the Federal Gazette and on their own website no later than one month after the half-year

concerned has ended, S2 (1) NetzDG. S 2 (2) NetzDG regulates the minimum aspects the report shall cover.

56. Furthermore, in accordance with S5 NetzDG, the provider of social networks shall appoint both a person authorised to receive service in the Federal Republic of Germany as well as a person in the Federal Republic of Germany authorised to receive information requests from German law enforcement authorities.

OTHER ISSUES RELATED TO HARMFUL DIGITAL COMMUNICATIONS

(i) Procedural Issues and Harmful Digital Communications

IRELAND

57. The Law Reform Commission of Ireland proposed in its Report on "Harmful Communications and Digital Safety" that in any prosecution for a harmful communications offence provided for in the Report, **the privacy of the person to whom the offence relates should be protected**, broadly by analogy with comparable provisions as to reporting restrictions in existing legislation (including their modification or removal), as well as providing for waiver by the person to whom the offence relates.[59] As in section 7 of the Criminal Law (Rape) Act 1981 Act, the Commission recommends that the accused should be able to apply to court for a direction to have the reporting restrictions removed and that the court must give such a direction if satisfied (a) that the direction is required for the purpose of inducing persons to come forward who are likely

[59] Para. 2.215 of the Report on "Harmful Communications and Digital Safety".

to be needed as witnesses at the trial, and (b) that the conduct of the applicant's defence at the trial is likely to be adversely affected if the direction is not given.

58. The Commission also proposes that **no prosecution for harmful communications offences should be brought against persons under the age of 17 years except by or with the consent of the Director of Public Prosecutions.**[60]

(ii) Jurisdictional Issues and Harmful Communications: Extraterritorial Effect

59. The internet is not limited to "a single geographical area nor is it neatly divisible along territorial boundaries into distinct local networks."[61] People may be subject to harmful communications from perpetrators, or through sites, located outside the State and, conversely, perpetrators based in the State may post harmful communications to or concerning individuals based outside it.

IRELAND

60. The Law Reform Commission of Ireland recommends[62] that **extraterritorial effect should apply to harmful communication offences**:
    - where a harmful communications offence is committed by a person in the State in relation to a means of communication located outside the State,
    - where a harmful communications offence is committed by a person outside the State in relation to a means of communication located in the State or

[60] Para. 2.218 of the Report on "Harmful Communications and Digital Safety".
[61] Biswas "Criminal liability for cyber defamation: jurisdictional challenges and related issues from Indian jurisprudence" (2013) CLTR 121, at 125.
[62] Para. 2.233 of the Report on "Harmful Communications and Digital Safety".

- where a harmful communications offence is committed by a person outside the State if the person is an Irish citizen, a person ordinarily resident in the State, an undertaking established under the law of the State, a company formed and registered under the Companies Act 2014 or an existing company within the meaning of the Companies Act 2014 and the offence is an offence under the law of the place where the act was committed.

(iii) Reform of Civil Remedies for Harmful Digital Communications

IRELAND

61. In Ireland, Individuals have the right under the Data Protection Acts 1988 and 2003[63] to **request the rectification and removal of personal data, which includes videos and images, from data controllers**. Where this request is not complied with, individuals can refer a complaint to the Office of the Data Protection Commissioner. The Acts also provide a separate means to obtain compensation against data controllers or processors for breach of a duty of care,[64] but this remedy is very difficult to obtain **as actual injury or damage must be proven before compensation is awarded.**[65] However, the 2016 General Data Protection Regulation provides for damages for "moral damage" or distress.

NEW ZEALAND

62. In July 2015, the New Zealand Parliament enacted the Harmful Digital Communications Act 2015. This Act was a response to a 2012 Report of the New Zealand Law Commission, which recommended reform of its laws on civil remedies to deal with harmful digital communications, including the need to establish an independent body

[63] https://www.dataprotection.ie/docs/Data-Protection-Acts-1988-and-2003:-Informal-Consolidation/796.htm
[64] Section 7 of the Data Protection Acts 1988.
[65] Michael Collins v FBD Insurance PLC [2013] IEHC 137.

with a remit to resolve harmful digital communications based complaints quickly through a mediation- type process. The 2015 Act provides that harmful digital communications complaints be made initially to an **"Approved Agency" to investigate and attempt to resolve them by advice, negotiation, mediation or persuasion.**[66] This body will also have a responsibility to provide education on policies for online safety and conduct on the Internet. If the Approved Agency fails to resolve the complaint, the Act provides that an individual may apply to the District Court for a number of civil orders which can be made against defendants and online content hosts. The Act also provides that **the court may make a declaration that a communication breaches a "communication principle", which would be intended primarily to have a persuasive effect on website hosts or internet service providers operating outside New Zealand.**

63. The Court can make one or more of the following types of orders against a defendant:

- an order to take down material, to refrain from the conduct concerned;
- an order not to encourage any other persons to engage in similar communications towards the affected individual;
- for a correction to be published;
- for a right to reply to be given to the affected individual and finally;
- for an apology to be published.[67]

In deciding whether or not to make an order, the Court is required to **take into account factors including the content of the communication and the level of harm caused or likely to be caused by it, the purpose of the communicator, the context, the age and vulnerability of the affected individual and whether the communication is in the public interest.**

[66] Sections 7 and 8 of the Harmful Digital Communications Act 2015.
[67] Section 19(1) of the Harmful Digital Communications Act 2015.

64. The civil enforcement regime introduced under the Harmful Digital Communications Act 2015 has the potential to **offer victims of harmful digital communications a quick and cost-effective means of obtaining civil remedies**. However, while the Approved Agency may have a valuable function in offering victims support and advice, it is unclear how effective mediation and similar methods may be in the online context. **Mediation may be an unsuitable response to harmful digital content because it takes time and most complainants will be focused on trying to get the content removed as quickly as possible.**

(iv) Civil Restraint Orders

IRELAND

65. In Ireland, section 10 (3) of the Non-Fatal Offences Against the Person Act 1997 enables the court to make a **restraining order restricting a person from communicating and/or approaching the victim where the person has been convicted of harassment**. In addition, section 10(5) of the 1997 Act **empowers a court to make such a restraining order even where the person has been acquitted of harassment**: "If on the evidence the court is not satisfied that the person should be convicted of an offence under subsection (1), the court may nevertheless make an order under subsection (3) upon an application to it in that behalf if, having regard to the evidence, the court is satisfied that it is in the interests of justice so to do." **A restraining order under section 10(3) cannot be made unless criminal proceedings have been taken against the alleged perpetrator of the harassment.**

66. The Law Reform Commission of Ireland recommends[68] that the power to issue a restraining order **should not be limited to instances where a criminal prosecution has been brought**. The Commission considers that individuals should be able to apply to the Circuit Court for civil restraining orders which would prevent, for such a period as the court may specify, a person from communicating by any means of communication with or about the individual or require that the respondent shall not approach within such distance as the court shall specify of the place of residence or employment of the individual seeking the order.

(v) Intermediary liability regime

GERMANY

67. On 1st October 2017, the German Netzwerkdurchsetzungsgesetz (Network Enforcement Act, NetzDG), entered into force[69]. The NetzDG is an "act to improve enforcement of the law in social networks", and **aims at combating fake news and hate speech**. The Act **establishes an intermediary liability regime**, through severe administrative penalties of up to 5 million euros, within time periods of 24 hours and 7 days respectively. As regulatory offences, it is possible for the maximum sanction to be multiplied by ten to 50 million euros.

68. Pursuant to Sec. 1(1) and (2) NetzDG, the "Act shall apply to telemedia service providers which, for profit-making purposes, operate internet platforms which are designed to

[68] Para 3.98 of the Report on "Harmful Communications and Digital Safety".
[69] https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/NetzDG_engl.pdf?__blob=publicationFile&v=2

enable users to share any content with other users or to make such content available to the public (social networks)" with more than 2 million registered users in Germany, regardless of where the social network is established.

69. **The law has been controversial in Germany** with some saying it could lead to inadvertent censorship or curtail free speech.[70] Indeed, though the Act does not create new content restrictions, it compels content removals on the basis of select provisions from the German Criminal Code. Many of these provisions raise serious freedom of expression concerns in and of themselves, including prohibitions on defamation of religion, **broad concepts of hate speech**, and criminal defamation and insult. Deputising private companies to engage in censorship on the basis of these provisions is deeply troubling according to some commentators, as they should not be criminal offences in the first place.[71]

(vi) Reporting obligations

GERMANY

70. According to the German Netzwerkdurchsetzungsgesetz (Network Enforcement Act, NetzDG), Social network providers which receive more than 100 complaints on unlawful content per calendar year are obliged to produce half-yearly reports on the handling of complaints about unlawful content on their platforms in German language. These reports shall be published in the Federal Gazette and on the social network's website. On the

[70] https://www.bbc.com/news/technology-42510868
[71] https://www.article19.org/wp-content/uploads/2017/09/170901-Legal-Analysis-German-NetzDG-Act.pdf

website, the report has to be easily identifiable, directly accessible and permanently available.

71. The reports shall cover the points stipulated in Sec. 2(2) NetzDG and *inter alia* comprise the criteria applied to decide **whether to delete or to block unlawful content, and the time between the receipt of complaints and the deletion / blocking**.

(B) CURRENT LEGAL FRAMEWORK IN MAURITIUS

72. The **Budapest Convention on Cybercrime**[72], which Mauritius has ratified[73], is the first international treaty seeking to address Internet and computer crime by harmonising national laws, improving investigative techniques, and increasing cooperation among nations. Its main objective, set out in the preamble, is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international cooperation. Many of its articles have been domesticated into our law.

Thus, article 2 on illegal access is transcribed at Sections 3 and 4 of the Computer Misuse and Cybercrime Act 2003. Article 3 on illegal interception can be found at Section 5 of the Computer Misuse and Cybercrime Act 2003. Article 4 entitled data interference is reproduced at Section 6 of the Computer Misuse and Cybercrime Act 2003. Article 5, pertaining to system interference is found at Section 7 of the Computer Misuse and Cybercrime Act 2003. Article 6 of the Convention on Misuse of devices is transcribed at

[72] https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561
[73] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=I6YOaKG1

Sections 8 and 9 of the Computer Misuse and Cybercrime Act 2003. Article 7 on Computer-related forgery is reproduced at Section 105A of our Criminal Code. Article 8 on Computer-related fraud is found under Section 10 of the Computer Misuse and Cybercrime Act 2003. Article 9 relating to Child pornography is echoed at Section 15 of The Child Protection Act 1994. Article 10 pertaining to infringement of copyright can be found at Section 56 of the Copyright Act.

FAKE NEWS

73. There are no laws in Mauritius which deal specifically with Fake news. Nevertheless, indirectly, we can find some provisions which incriminate the propagation of false information.

74. Thus, according to Section 46(g) of the **Information and Communication Technologies Act 2001**,[74] it is an offence to knowingly sends, transmits, or cause to be transmitted a **false or fraudulent message**. Section 46 (ga)[75] makes it an offence for anyone who "uses telecommunication equipment to send, deliver or show a message which is obscene, indecent, abusive, threatening, **false or misleading**, or is likely to cause distress or anxiety". And according to Section 46 (na), commits an offence anyone who "knowingly provides **information which is false or fabricated**".

[74] The object of this Act is to provide for the establishment and management of an Information and Communication Technologies Authority; the regulation of the information and communication technologies sector including telecommunications, the use of the internet, the enhanced development of an information society and online services, the protection and security of data, the facilitation of convergence; and the establishment of ICT Advisory Council and of an ICT Appeal Tribunal; the democratisation of information and communication technologies for the promotion of a knowledge-based society; and finally the transition towards a fully liberalised and competitive market in the information and communication sector.

[75] Section 46(ga) was included by the Information Communication Technology Amendment Bill (No. XXI of 2016).

75. Fake news can also be covered under the defamation Section of our Criminal Code. Indeed, according to Section 282 of the Criminal Code:

"*(1) Any imputation or allegation of a fact prejudicial to the honour, character or reputation of the person to whom such fact is imputed or alleged is a defamation.*
(2) Any imputation or allegation concerning the honour, character or reputation of a deceased person is a defamation where it is calculated to throw discredit on or be hurtful to the feelings of the family or relatives of the deceased.
(3) Any person who, by ***any of the means specified in section 206****, is guilty of defamation shall be liable to imprisonment for a term not exceeding 5 years and a fine not exceeding 50,000 rupees.*"

76. Since the amendment brought by the **Judicial and Legal Provisions Act (Act No. 3 of 2018)**,[76] Section 206 which is referred to in Section 282, the modes of commission of the offence are by any writing which is sold, put up for sale, published, distributed, posted up, circulated, exhibited, exposed, broadcast or transmitted in any public place, public meeting or procession. And the new Section 206 (3) provides that:

"In *this section –*
"broadcast" means using radio communication, whether by sound or vision, for reception by members of the public;
"electronic" means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic or similar capabilities;
"writing" –
(a) means any newspaper, pamphlet, drawing, engraving, picture, illustration, placard, handbill, emblem, image, printed matter or any other written work; and
(b) includes –
(i) any writing by electronic means; or
(ii) any communication, whether in the form of speech or other sound."

[76] In the view of enhancing digital safety on the internet, the Judicial and Legal Provisions Act has been passed in parliament in March 2018.

FAKE PROFILES

77. Those who set up Fake profiles can sometimes be prosecuted under the offence of swindling. Indeed, according to **Section 330 of our Criminal Code** concerning swindling, it is provided, in subsection (1) that:

"Any person who, by using a fictitious name, or assuming a false character, or by employing fraudulent pretences, to establish the belief of the existence of any fictitious operation or of any imaginary power or credit, or to create the expectation or apprehension of any success, accident or other chimerical event, or who, by means of a cheque drawn on any banker in Mauritius to the order of any person or to bearer, for the payment of which there is insufficient provision at the time of the presentment thereof, obtains the remittance or delivery of any funds, movable property, obligation, condition, bill, acknowledgement, acquittance or discharge, and by any such means as aforesaid, swindles another person out of the whole or of a part of his property shall be punished by penal servitude for a term not exceeding 20 years, and by a fine not exceeding 150,000 rupees."

78. **Section 46 (na) of the ICTA** could also cover fake profiles as it provides for "knowingly provides information which is false or fabricated". Moreover, **Section 46 (h) (ii) is drafted in terms broad enough so as to cover the situation of fake profiles**: "*uses, in any manner other than that specified in paragraph (ga), an information and communication service, including telecommunication service, - for the purpose of causing annoyance, inconvenience or needless anxiety to any person*".

79. Fake profiles could also fall under Section 6 of the **Computer Misuse and Cybercrime Act 2003**. According to the said Section, subject to subsections (3) and (4), any person who, knowingly does an act which causes **an unauthorised modification of data** held in any computer system shall, on conviction be liable to a fine not exceeding 100,000 rupees and to penal servitude for a term not exceeding 10 years.

But the offence would not be constituted if the author of the fake profile set one up from scratch instead of gaining access to someone's else profile and then modify it.

80. Fake profiles could likewise be covered by **Section 5 of the Computer Misuse and Cybercrime Act 2003** entitled "**Unauthorised access to computer data**", any person who causes a computer system to perform a function, **knowing that the access he intends to secure is unauthorised**, shall commit an offence and shall, on conviction, be liable to a fine not exceeding 50,000 rupees and to penal servitude for a term not exceeding 5 years.

The Intermediate Court considered, in ***Police v Mohamad (2011) INT 120***, that: "the insertion of an ATM card in the facility and the keying-in of a PIN code in respect of debit of an account is a 'function' that creates a pathway 'access' to data that would have been otherwise been protected and/or 'makes use of any of the resources of the computer system' and it is the function leading to access that causes money to be debited from a person's account. Indeed, it is the unlawful act of causing a computer system to perform the function coupled with the knowledge that such access is unauthorized that is punishable and not necessarily the withdrawal of money per se."

In ***Ramsaran v State of Mauritius (2013) SCJ 446***, it was held that: "it is clear that an offence is committed under Section 3(1) of the Act, on each occasion that a person causes a computer system to perform a function, knowing that the use he intends to make is unauthorised. It shall be unauthorized where there is no consent given to the user, from the person entitled to give consent, to make use of the computer system in order to perform a function of the kind in question. It is plain therefore, that an offence would lie against the appellant on each occasion that he has had access to the ATM to make a withdrawal without the consent of the complainant who was the only person entitled to

give him consent to access the system in order to make a withdrawal of money from her account by making use of her card."

Lacunae

81. The provision on swindling would be of no use to incriminate the setting up of a fake profile if the person who uses a fictitious name or assumes a false character does so but not to "swindle another person out of the whole or of a part of his property", but only, for example, to damage his reputation.

82. As to Section 46 (h) (ii), one of its shortcomings is that the prosecution will have to prove that annoyance is caused or is likely to be caused, which can be hard to show, but this is a prerequisite of the said provision, as has been said in ***Lokee v The State (2010) SCJ 378*** that "*It is an essential element of the offence that the messages sent caused annoyance to a person*".

83. The absence of an offence of "indirect harassment", which the Ireland Law Reform Commission recommended to make room for in its 2013 Report on Aspects of Domestic Violence, does not allow to prosecute those who create fake profiles and by doing so, indirectly cause distress and anxiety to someone.

84. Thus, in Mauritius, there is no offence linked directly to the fact that a fake profile is being set up, and which would be of strict liability.

OTHER HARMFUL DIGITAL COMMUNICATIONS

Direct harassment

85. Direct harassment is not targeted as such in the provisions of our laws.

86. Nevertheless, **Sections 46 (ga) and (h) of the ICTA** could be used to incriminate online harassment. Indeed, according to Section 46 (ga), commits an offence anyone who "uses telecommunication equipment to send, deliver or show a message which is obscene, indecent, abusive, threatening, false or misleading, or is likely to cause distress or anxiety", while Section 46 (h) provides that someone commits an offence if he "uses, in any manner other than that specified in paragraph (ga), an information and communication service, including telecommunication service, - (i) for the transmission or reception of a message which is grossly offensive, or of an indecent, obscene or menacing character; or (ii) for the purpose of causing annoyance, inconvenience or needless anxiety to any person"

87. In ***Sujeeun v The State (2018) SCJ 165***, the Supreme Court compared Section 46 (h) (ii) with section 127 of the UK Communications Act 2003: "*In DPP v/s Collins [2006] 1 WLR, the respondent was prosecuted for the offence of sending, by means of a public electronic communications network, messages that were grossly offensive, contrary to section 127(1)(a) of the Communications Act. On appeal it was held that "the offence was complete when the message was sent; that it was for the Court, ..., to determine as a question of fact whether the message was grossly offensive; that it was necessary to show that the defendant intended his words to be grossly offensive to those to whom the message related, or that he was aware that they might be taken to be so; that the*

defendant's messages were grossly offensive and would be found by a reasonable person to be so". An analogy can be drawn between section 127 of the UK Communications Act 2003 and our section 46(h) of the ICTA."

Lacunae

88. The Offence of "Moral harassment", which could be used to incriminate online harassment does not presently exist in our Criminal Code[77]. The latter talks only about "Sexual harassment" at Section 254.

Stalking

89. Contrarily to Scotland, there are no provisions in our law which explicitly incriminate stalking.

90. Nevertheless, Section 46 (h) (ii) of the ICTA, which provides that anyone who uses, in any manner other than that specified in paragraph (ga), an information and communication service, including telecommunication service for the purpose of causing annoyance, inconvenience or needless anxiety to any person commits an offence could be used to prosecute certain forms of stalking.

Lacunae

91. Certain forms of stalking would not fall under Section 46 (h) (ii) of the ICTA, for example, the fact of monitoring the use by the victim of the internet.

[77] Contrarily to what can be found in the French Penal Code

Offences Designed to Target Once-off Harmful Digital Communications

92. Behaviors listed under Section 46 (ga) and 46 (h) of the ICTA would be incriminated even though they occurred only once, like is witnessed by the use of the term "message" in singular form.

Threats, Intimidation and Offensive Messages

93. Sections 46 (ga) and 46 (h) (i) and (ii) allow for the prosecution of those who send threats and offensive messages over the internet and who try to intimidate their victims.

Incitement

94. Section 46 (ga) and Section 46 (h) (ii) of the ICTA could be used to incriminate the fact that some persons, due to the anxiety and distress caused by some messages be sent to them, are susceptible to be incited to endanger their own lives.

Lacunae

95. There are no provisions, however, in our legislation which would make it an offence for someone to incite another person to commit suicide, which the Law Commission of New Zealand recommends.

Grooming

96. Our Criminal Code only sanctions those who try to debauch youth (Section 251) and those who have sexual intercourse with minors (Section 249 (4)).

Lacunae

97. There are no provisions which make it an offence to make sexual proposals to a minor.

Offence of distributing a threatening false, indecent or obscene message

98. **Section 46 (ga) of the ICTA**, according to which anyone who "uses telecommunication equipment to send, deliver or show a message which is obscene, indecent, abusive, threatening, false or misleading, or is likely to cause distress or anxiety" commits an offence, can be relied upon to prosecute those who send obscene messages on social media for example.

    It is to be noted that it is a strict liability offence and that consent of the other party who receives the said message would not be a defence. The main shortcoming of this provision is the definition to be given to the word "obscene".

99. The **Criminal Code (Supplementary) Act, in its Section 86**[78], incriminates dealing with "Obscene matter". Here again, the problem which arises, is the definition to be relied

[78] Dealing in obscene matter
(1) Any person who –
(a) for the purposes of, or by way of, trade or for distribution or public exhibition, makes or produces or has in his possession any obscene matter;
(b) for a purpose specified in paragraph (a), imports, conveys, or exports or causes to be imported, conveyed or exported any obscene matter or in any manner puts into circulation any obscene matter;
(c) carries on or takes part in a business, whether public or private, concerned with any obscene matter or deals in any obscene matter in any manner, or publicly distributes or exhibits or makes a business of lending any obscene matter; or
(d) advertises or makes known by any means that a person is engaged in any of the acts specified in paragraphs (a) to (c), or advertises or makes known how or from whom the obscene matter can be procured either directly or indirectly, shall commit an offence and shall, on conviction, be liable to a fine not exceeding 100,000 rupees and to imprisonment for a term not exceeding one year and the obscene matter forming the subject matter of the offence shall be forfeited.
(2) (a) Any person who sells, lends, hires or distributes to a minor or exposes or allows to be exposed to the view of a minor any obscene matter shall commit an offence and, notwithstanding section 152 of the Criminal Procedure Act, shall, on conviction, be liable to imprisonment for a term not exceeding 4 years together with a fine not exceeding 100,000 rupees.

upon when interpreting what exactly constitutes "obscene". In ***Desvaux de Marigny J. J. J. R v The State (1999)* SCJ 414**, the Supreme Court said: "*As the law stands, the word "obscene" to be found in section 86(1)(c) of the Criminal Code (Supplementary) Act is to be given its dictionary meaning, that is "indecent especially grossly or repulsively so lewd, tending to deprave or corrupt, highly offensive, morally repugnant" according to the Concise Oxford Dictionary and* "Qui révolte, offense ouvertement la pudeur; qui présente un caractère très choquant de crudité et de trivialité" according to Le Robert, Dictionnaire de la langue française". In its *obiter*, the Court highlighted that: "*There is indeed a school of thought that adults, as opposed to minors, should no more be prevented access to materials which in the opinion of many are likely to deprave and corrupt, so long as they exercise their freedom in private.*"

Lacunae

100. The use of the words "*obscene*" and "*indecent*" in Sections 46 (ga) and (h) (i) of the ICTA could make it possible to prosecute consensual sharing of intimate images between adults.

Distribution of Intimate images

101. According to **Section 15 of the Child Protection Act,** entitled "Indecent photographs of children":

(b) Part X of the Criminal Procedure Act and the Probation of Offenders Act shall not apply to a person liable to be sentenced under paragraph (a).
(3) In this section, "obscene matter" means any obscene writing, drawing, print, painting, printed matter, picture, poster, emblem, photograph, cinematograph film, video tape, slide, data stored on a computer disc or by any other electronic means capable of conversion into a photograph or any other obscene object.
(4) In addition to making an order that the obscene matter forming part of the subject matter of the offence be forfeited, the Court shall, where appropriate, order that the obscene matter be no longer stored on and made available through the computer system, or that the material be deleted.

"(1) Any person who
(a) takes or permits to be taken or to make, any indecent photograph or pseudo photograph of a child;
(b) distributes or shows such indecent photograph or pseudo-photograph;
(c) has in his possession such indecent photograph or pseudo-photographs, with a view to it being distributed or shown by himself or any other person; or
(d) publishes or causes to be published any advertisement likely to be understood as conveying that the advertiser distributes or shows such indecent photograph or pseudo photograph, or intends to do so, shall commit an offence.
(2) Where a person is charged with an offence under subsection (1)(b) or (c), it shall be a defence for him to prove that
(a) he had reasonable grounds for distributing or showing the photograph or pseudo photograph or having them in his possession; and
(b) that he had not himself seen the photograph or pseudo-photograph and did not know, nor had any cause to suspect, it to be indecent.
(3) Where -
(a) the impression conveyed by the pseudo-photograph is that the person shown is a child; or
(b) the predominant impression conveyed is that the person shown is a child, notwithstanding that some of the physical characteristics shown are those of an adult, the pseudo-photograph shall be treated for all purposes of this Act as showing a child."

102. A child targeted in this section is an unmarried person under the age of 18. Also, indecent photograph is defined as including an indecent film, a copy of an indecent photograph or film, and an indecent photograph comprised in a film. As per the act photograph includes the negative as well as the positive version and data stored on a computer disk or by other electronic means[79] which is capable of conversion into a photograph. And finally, a pseudo photograph means an image, *whether made by computer graphics or by any other means*, which appears to be a photograph.

[79] *Police v Bahadoor* (2012) INT 209.

Lacunae

103. While in the New Zealand Harmful Digital Communications Act 2015, the mere taking of an intimate image without the consent of the other person is incriminated, it is not the case in the ICTA, as witnessed by the use of the terms "send, deliver or show" in Section 46 (ga) or "transmission or reception" in Section 46 (h).

104. Furthermore, nothing in the Child Protection Act prevents someone from consulting child pornographic websites, while it is the case in France for example.

Hate Speech

105. The **Judicial and Legal Provisions Act (Act No. 3 of 2018)** repeals and replaces Section **282 of our Criminal Code** in a view of making the internet and social media platform safer to users by using preventive tools against the stirring of racial hatred. The new section 282 of our Criminal Code provides as follows:

"*(1) Any person who, with intent to stir up contempt or hatred against any section or part of any section of the public distinguished by race, caste, place of origin, political opinion, colour, creed or sex –*

(a) publishes, distributes, posts up, circulates, exhibits, exposes, broadcasts or transmits any writing which is threatening, abusive or insulting; or

(b) uses any word or makes any gesture in any public place, public meeting or procession which is threatening, abusive or insulting, shall commit an offence and shall, on conviction, be liable to penal servitude for a term not exceeding 20 years and to a fine not exceeding 100,000 rupees.

(2) Any writing or any copy of such writing in respect of, or in connection with, which an offence has been committed under this section shall be forfeited and destroyed, or deleted, as the case may be."

106. It is to be noted that the meaning of broadcast and electronic in the proposed Section 282 of our Criminal Code is similar to the proposed Section 206 as elaborated upon above. Hence, those proposed amendments to our Criminal Code are a clear response to the rise in the racial and dangerous contents posted on Social Media and other platforms. Therefore, one can note that the legislator has a clear intent of enhancing digital safety to users of social media and other platforms on the internet.

107. Moreover, Section 46 (ga) of the ICTA, according to which commits an offence anyone who "uses telecommunication equipment to send, deliver or show a message which is obscene, indecent, abusive, threatening, false or misleading, or is likely to cause distress or anxiety", could also be used to prosecute those guilty of hate speeches.

CIVIL REMEDIES

Rectification and removal of personal data

108. Similarly, to the Irish Data Protection Acts 1988 and 2003, our **Data Protection Act 2017** provides, in its Section 37 (2) (e), that where personal data are being processed, the controller shall provide to the data subject information relating to the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to the processing of the data.

Court orders

109. Presently, in our laws, contrarily to the Ireland Non-Fatal Offences Against the Person Act 1997, Courts cannot make orders to restrain someone from contacting another person if the latter has not been found guilty of an offence.

(C) REFORM PROPOSALS

FAKE NEWS

110. We have seen, from experiences discussed above, that when specific pieces of legislation have been passed which target fake news, they have been met with harsh criticisms, as was the case in Germany, France, or Malaysia, the two latter even seeing the said laws be repealed.

111. The main danger to enact such legislation is that it poses a threat to freedom of expression, as it can be used, among other things, to gag dissenting voices. Indeed, decreeing a legal duty of "truth" would create a dangerous instrument to control journalistic activities: allowing public officials to decide what amounts to truth is equivalent to accepting that the forces in power have a right to silence views they disagree with, or beliefs they do not share. Such laws can preclude the discussion of ideas which challenge the norm, restraining public debate and restricting criticism of societal attitudes or of those in power. Under such laws, journalists or human rights activists could be sent to prison on accusations of disseminating untrue statements about alleged wrongdoings.

112. Moreover, from a practical standpoint, Germany, before passing its law, had to the agreements of large social network companies to work with them to some degree, with the Big Three social media companies - Facebook, Twitter, and YouTube - now setting up legal compliance offices for Network Enforcement Act (NEA). Also, Facebook in Germany has hired more than 1,000 content moderators to ensure the timely removal of illegal content reported to it. All these could be difficult to put in place in Mauritius.

113. When fake news poses immediate threats, these are already addressed in our law, for example, by **Section 101 of the Criminal Code (Supplementary) Act relating to "Raising false alarm of fire"[80] or Section 102 of the same Act pertaining to "Bomb Hoaxes".**[81]

[80] Raising false alarm of fire
(1) Any person who in any manner knowingly gives or causes to be given a false alarm of fire to any fire brigade or to any officer thereof, shall commit an offence and shall, on conviction, be liable to a fine not exceeding 100,000 rupees.
(2) Any person who commits an offence under subsection (1) may be prosecuted either by the Police or by a municipal officer or by an officer of any municipal council.

[81] Bomb hoaxes
(1) Any person who –
(a) places any article or explosive in any place whatsoever;
(b) dispatches any article or explosive by post or otherwise,
with the intention of inducing in some other person a belief that a bomb is likely to explode, shall commit an offence.
(2) Any person who communicates any information which he knows or believes to be false to another person with the intention of inducing in him or any other person a false belief that a bomb or other explosive is lying in certain premises and liable to explode shall commit an offence.
3) Any person who commits an offence under this section shall be liable, on conviction, to imprisonment for a term not exceeding 10 years and to a fine not exceeding 100,000 rupees.
(4) For the purposes of this section "explosive" has the same meaning as in section 58.

Recommendation

114. For all these reasons, the Commission does not consider it appropriate that a specific law be enacted to deal with fake news.

FAKE PROFILES

115. As we have seen above, the offence of swindling under Section 330 of the Criminal Code is inefficient to tackle fake profile or identity theft if the author does not do so to swindle one's property. Neither would Section 10 of the Computer Misuse and Cybercrime Act 2003 entitled "Electronic Fraud"[82] would be of any use here, as "loss of property" is an essential element of the offence.

[82] "Electronic fraud
Any person who fraudulently causes loss of property to another person by-
(a) any input, alteration, deletion or suppression of data; or
(b) any interference with the functioning of a computer system,
with intent to procure for himself or another person, an advantage, shall commit an offence and shall, on conviction be liable to a fine not exceeding 200,000 rupees and to penal servitude for a term not exceeding 20 years."

Recommendation

116. The Commission thus proposes to add a new **Section 369C in our Criminal Code entitled "Digital usurpation of identity"**[83] which would read as follows:

"*The act of impersonating a third party or make use of one or more data of any kind which allows to identify him in view of disturbing his tranquillity or that of others, or harm his honour or his reputation or consideration, is punishable by imprisonment and a fine not exceeding 150 000 rupees.*

This offense is punishable by the same penalties when committed on a public online communication network."

117. The above provision would allow for the prosecution of those who set up fake profiles.

118. The legal result is obtained by identity theft alone or by the mere use of data of any kind to identify a third party. It is therefore situated upstream of the dreaded result, which makes the offense a formal one. The mental element consists of the necessity to establish the conscious will of the author to impersonate a third party or to use data of any kind to identify it. It is also necessary to establish the conscious intention of the

[83] Based on Article 226-4-1 of the French Penal Code.

author to undermine the tranquility, honor or consideration of the victim. The offense is an instantaneous one.

119. The Commission is of the view that only impersonation of third parties should be criminalised and not the fact of setting up a fake profile of an inexistent person. Indeed, for some reasons, people might want to stay anonymous when posting certain information, for example, when reporting a crime, so as to avoid reprisals. Nevertheless, the fact of setting up a fake profile of an inexistent person, in view of swindling someone's property would constitute an offence under Section 330 of our Criminal Code.

ONLINE HARASSMENT

120. The New Zealand Law Commission considers, in its report on Harmful Digital Communications, that there should be an offence of sending an offensive message with intent to cause distress.

121. According to **Section 46 (ga) of the ICTA**, anyone who uses telecommunication equipment to send, deliver or show a message which is obscene, indecent, abusive, threatening, false or misleading, or is likely to cause distress or anxiety commits an offence.

122. Moreover, according to **Section 46 (h) of the ICTA**, any person who uses, in any manner other than that specified in paragraph (ga), an information and communication service, including telecommunication service, for the transmission or reception of a message which is grossly offensive, or of an indecent, obscene or menacing character; or for the purpose of causing annoyance, inconvenience or needless anxiety to any person commits an offence.

123. Although these provisions might cover some cases of online harassment, they might fall short of some instances to incriminate conducts which are obviously antisocial.

Recommendation

124. In the Interim Report on Reform of Criminal Code dated May 2016, it has been suggested to introduce a **new Section 255 dealing with Moral harassment.**[84]

Thus, according to Subsection (1), harassing another person by repeated conduct which is designed to or which leads to a deterioration of his work conditions likely to violate his rights and his dignity, to damage his physical or mental health or compromise his career prospects, shall be punished by imprisonment for a term not exceeding two years and a fine not exceeding 100,000 rupees.

While Subsection (2) provides that to harass a person by repeated words or conduct which have as object or as effect the degradation of the living conditions resulting in impaired physical or mental health shall be punished by imprisonment for a term not exceeding one year and a fine not exceeding 50,000 rupees when these acts have caused a total incapacity for work below or equal to eight days or resulted in no disability.

It is also expressly provided that constitutes an aggravating circumstance the fact that the offence is committed by the use of a communication service to the public online.

[84] Based on articles 222-33-2 to 222-33-2-2 of the French Penal Code.

125. In the light of the new Section proposed, we see that the terms "*repeated words or conduct which have as object or as effect the degradation of the living conditions resulting in impaired physical or mental health*" will encompass more behaviors than those used in the ICTA.

126. Nevertheless, for the new offence of moral harassment to be constituted, the conduct or words of the author must be repeated, which does not allow to target Once-off Harmful Digital Communications. But **Sections 46 (ga) and (h) of the ICTA does not require repeated messages to be sent** and thus would allow the constitution of the offence by the sending of only one message.

STALKING

127. Stalking should be distinguished from harassment, stalking being an "an aggravated form of harassment characterised by repeated, unwanted contact that occurs as a result of fixation or obsession and causes alarm, distress or harm to the victim. This element of intense obsession or fixation, which creates an unwanted intimacy between the stalker and the victim, differentiates stalking from harassment."[85]

128. We consider that harassment and stalking, though having some elements in common, are quite different in nature and thus proposes that a new offence of stalking be introduced in the Criminal Code. Indeed, the offence of "Moral Harassment" which is

[85] Para. 2.23 of the Report by the Law Reform Commission of Ireland. It thus recommends that a specific offence of Stalking be introduced based on the Criminal Justice and Licensing Scotland Act 2010.

being proposed in the Interim Report would not cover all the conducts linked with stalking.

Recommendation

129. Consequently, the **Commission recommends that a new Section 255A[86] be introduced in the Criminal Code**, and which would read as follows:

"*255A Stalking*

(1) Stalking another person shall be punished by imprisonment for a term not exceeding five years and a fine not exceeding 100,000 rupees.

(2) For the purposes of subsection (1), stalking takes place where—

(a) the author engages in a course of conduct,

(b) subsection (3) or (4) applies, and

(c) the author's course of conduct causes the victim to suffer fear or alarm.

(3) This subsection applies where the author engages in the course of conduct with the intention of causing the victim to suffer fear or alarm.

(4) This subsection applies where the author knows, or ought in all the circumstances to have known, that engaging in the course of conduct would be likely to cause the victim to suffer fear or alarm.

(5) It is a defence for a person charged with an offence under this section to show that the course of conduct—

(a) was authorised by virtue of any enactment or rule of law,

[86] Based on Section 39 of the Scotland Criminal Justice and Licensing (Scotland) Act 2010.

(b) was engaged in for the purpose of preventing or detecting crime, or

(c) was, in the particular circumstances, reasonable.

(6) In this section---

"conduct" means---

(a) following the victim,

(b) contacting, or attempting to contact, the victim by any means including through electronic means of communication,

(c) publishing any statement or other material—

(i) relating or purporting to relate to the victim,

(ii) purporting to originate from the victim,

(d) monitoring the use by the victim of the internet, email or any other form of electronic communication,

(e) entering any premises,

(f) loitering in any place (whether public or private),

(g) interfering with any property in the possession of B or of any other person,

(h) giving anything to the victim or to any other person or leaving anything where it may be found by, given to or brought to the attention of the victim,

(i) watching or spying on the victim,

(j) acting in any other way that a reasonable person would expect would cause the victim to suffer fear or alarm, and

"course of conduct" involves conduct on at least two occasions."

ONLINE INCITEMENT

130. The Law Commission of New Zealand considers in its above quoted Paper, that there is no need to create a specific offence of inciting offensive communication but recommends making incitement of suicide in itself criminal.

Recommendation

131. In its Interim Report on Reform of the Criminal Code, the Law Reform Commission proposed to incriminate, in a **new Section 239C, incitation to suicide.**[87] Thus, inciting another person to commit suicide shall be punished by imprisonment for a term not exceeding five years and a fine not exceeding 150,000 rupees where the incitement was followed by suicide or attempted suicide (subsection 1 (a)), and Propaganda or advertising, **in whatever manner**, in favour of products, articles or methods recommended as means to procure one's death, shall be punished by imprisonment for a term not exceeding three years and a fine not exceeding 150,000 rupees (subsection (2)).

132. With regard to the material element, the provocation must have been followed by effect, whether the suicide was actually carried out or simply attempted. It is a material

[87] Based on articles 223-13 and 223-14 of the French Penal Code.

offense, which implies its rejection in case of voluntary withdrawal *in extremis* of the person prone to suicide. The provocation must target a specific person, even a collective one. The simple advice to commit suicide is not sufficient for constituting the offense; thus, providing a knife to a person whose suicidal and unbalanced behavior is known, and challenging him to use it, does not have a binding or convincing character that can paralyze the will by leaving no other alternative than death.

133. However, if no suicide or attempt to suicide has been made, the author of **such incitement could still be prosecuted on the basis of Section 46 (ga) or (h) of the ICTA for causing anxiety, distress or annoyance to the victim**.

134. While in the provocation to suicide *stricto sensu* (subsection (1)), we penalize a direct and personal connection by provocation, in the second offense of subsection (2) we incriminate the indirect and impersonal link (by advertising) between the message and the suicide. In other words, unlike the offense covered by subsection (1), here the act of propaganda or publicity implies a general broadcast to the public, and not to a particular person.

Propaganda or publicity must, in order to be punishable, be in favor of products, objects or methods recommended as means of killing oneself. These means will, most often, consist of the enumeration of toxic products, in particular of medicinal substances, with an indication of their lethal doses, but incrimination also encompasses all other means of terminating one's life. It does not matter the greater or less efficiency of the means indicated. The content of the advertisement or propaganda must be sufficiently precise and give concrete "tips" allowing a person to commit suicide.

Contrary to the provocation to suicide referred to in subsection (1), advertising of means of killing oneself is a formal offense, that is to say, it is constituted whether it has or not been followed by effect. In fact, it does not matter whether the person has attempted to commit suicide by resorting to the means advocated by the advertising action, since it is this advertising itself which, because of the potential danger that it constitutes, is incriminated.[88]

[88] For a more elaborate discussion about these new provisions, see Discussion Paper « Reform of Law on Endangering Persons in the Criminal Code » (April 2018).

GROOMING

135. In its Paper on "Harmful Digital Communications: the adequacy of the current sanctions and remedies", the New Zealand Law Commission recommends enacting a provision that makes the process of grooming criminal in itself, even though no overt act has been done in preparation for a meeting. In its Review Paper on Criminal Protection of Children's Rights (May 2016), we also recommended that Grooming should be made an offence.[89]

Recommendation

136. In the Interim Report on the Reform of the Criminal Code (May 2016), it has been proposed to repeal and replace Section 251[90] of the Criminal Code about **"Debauching Youth"** and to introduce **a new Section 251A entitled "Sexual proposals by way of an electronic means of communication to a minor under 16 years of age"**.[91]

According to the new Section 251:

"*(1) Promoting or attempting to promote the corruption of a minor shall be punished by penal servitude for a term not exceeding ten years.*

The penalty shall be increased to penal servitude for a term not exceeding fifteen years where the minor is under sixteen years of age, where the minor was put in contact with the offender by the use, for the dissemination of messages to an

[89] See pg. 61 of the Review Paper.
[90] Based on article 227-22 of the French Penal Code.
[91] Based on article 227-22-1 of the French Penal Code.

unrestricted public, of a telecommunications network, or where the offence is committed inside an educational institution or, in the vicinity of an educational institution at a time when the pupils or the public are entering or leaving such an institution.

(2) The same penalties shall be applicable when an adult organises a meeting involving indecent sexual exposure or sexual relations at which minors are present or are participating or knowingly attends such meeting.

The penalties shall be increased to penal servitude for a term not exceeding twenty years where the offence was committed by an organised band or in relation to minors less than sixteen years of age."

137. The new Section 251A would provide the following:

"*(1) An adult who makes sexual proposals to a minor under sixteen years of age or someone posing as such by using an electronic means of communication shall be punished by imprisonment for a term not exceeding five years and a fine not exceeding 100,000 rupees.*

(2) These penalties shall be increased to imprisonment for a term not exceeding seven years and a fine not exceeding 150,000 rupees when the proposals were followed by a meeting."

138. The new Section 251 makes it an aggravating circumstance to promote or attempt to promote the corruption of a minor[92] by using a telecommunication network.

139. As to the new Section 251A, this new incrimination reflects the contemporary concern of combating the dangers resulting for minors from the use of modern means of telecommunications, especially the Internet, and which is not covered presently by our laws. The offense is constituted only when the sexual propositions were made by an adult to a minor of less than sixteen using a means of electronic communication. It is therefore clearly in view to prevent pedophile behavior on the internet by discouraging any adult to use an electronic means of communication to identify and contact a minor of less than sixteen for the purpose of sexually abusing him.

140. These two new above-mentioned provisions would allow to fight efficiently against grooming.

[92] According to French doctrine, corruption of minor is "when an individual strives to take advantage of the youth and the inexperience of his victim to initiate him to a vice, and to try to make him slave to it." Jean-Paul Doucet, « Corruption de mineur » [archive], Dictionnaire de droit criminel, 2014.

INTIMATE IMAGES

141. As has been seen above, New Zealand criminalizes the publication of intimate images by the person who made the image, without the consent of the person depicted.

142. Section 46 (ga) of the ICTA, according to which anyone commits an offence if he "uses telecommunication equipment to send, deliver or show a message which is obscene, indecent, abusive, threatening, false or misleading, or is likely to cause distress or anxiety", and Section 46 (h) (i), which makes it an offence for a person to use "in any manner other than that specified in paragraph (ga), an information and communication service, including telecommunication service, for the transmission or reception of a message which is grossly offensive, or of an indecent, obscene or menacing character", would allow for the prosecution of intimate images.

Recommendation

143. So as not to incriminate the consensual sharing of intimate images (commonly referred to as "sexting"[93]) between adults,[94] it is proposed to delete the words "*obscene*" and "*indecent*" in Section 46 (ga) and the words "obscene" and "indecent" (h) (i). Moreover, these words could be opened to constitutional challenge to their vagueness.[95] Despite the deletion of these words, the provision would allow for the prosecution of sharing intimate images taken with consent but shared without consent[96], as this would undoubtedly cause "distress and anxiety".

144. Nevertheless, the mere taking of an intimate image without the consent of the other person is not incriminated, as witnessed by the use of the terms "send, deliver or show" in Section 46 (ga) or "transmission or reception" in Section 46 (h).

[93] "Sexting occurs when individuals share explicit images of themselves over the mobile phones or across social networks. It is common, almost a trend for our teenagers, especially girls, to send explicit photos of themselves to their boyfriends. If the relationship turns sour, as is often the case, the explicit photograph is circulated to school / college friends or simply posted on a social media page online." DPP E-Newsletter, Issue 39, August 2014, p. 3.

[94] Thus in the UK, there is no offence if it's a sexually explicit picture/image of an adult and sent between adults: https://www.psni.police.uk/contentassets/fae34aff4af6409e9ad393130043ec55/sexting__the_law_leaflet_trifold.pdf

[95] Based upon Para. 2.191 of the Ireland Report on Harmful Communications and Digital Safety.

[96] As proposed by the New Zealand Law Commission at Para. 4.94 of the report on Harmful Digital Communications.

Recommendation

145. Thus, it is recommended to add a **new Section 46B to the ICTA**, to be entitled **"Taking and distributing of intimate visual recording without consent"** which would read as follows:

"*(1) Any person who takes an intimate visual recording of another person without his consent commits an offence and shall, on conviction, be liable to a fine not exceeding 1,000,000 rupees and to imprisonment for a term not exceeding 5 years."*

(2) The offence defined under subsection (1) shall be punished by penal servitude for a term not exceeding fifteen years.

1° where it is committed on a minor of less than 16 years;

2° where it is committed by a legitimate, natural or adoptive ascendant, or by any other person having authority over the victim;

3° where it is committed by a person misusing the authority conferred by his functions;

4° where it is committed by two or more acting as authors or accomplices;

5° where it is committed with the use or threatened use of a weapon.

6° when the victim was brought into contact with the author through the use, for the dissemination of messages to an unrestricted public, of an electronic communications network;

7 ° where it is committed by the spouse or partner of the victim;

8 ° where it is committed by a person acting under clear influence of alcohol or

under the obvious influence of drugs;

9 ° where it is committed in the exercise of this activity, on a person engaged in prostitution, including occasionally.

(3) The threat to publish an intimate visual recording taken even with consent shall be punishable by imprisonment.

(4) Any person who publishes an intimate visual recording without consent of the party depicted in the recording, taken even with consent, shall be punishable by penal servitude for a term not exceeding 20 years.

(5) For the purpose of this Section, intimate visual recording[97]*—*

(a) means a visual recording ***(for example, a photograph, videotape, or digital image)*** *that is made in any medium using any device with or without the knowledge or consent of the individual who is the subject of the recording, and that is of—*

(i) an individual who is in a place which, in the circumstances, would reasonably be expected to provide privacy, and the individual is—

(A) naked or has his or her genitals, pubic area, buttocks, or female breasts exposed, partially exposed, or clad solely in undergarments; or

(B) engaged in an intimate sexual activity; or

(C) engaged in showering, toileting, or other personal bodily activity that involves dressing or undressing; or

(ii) an individual's naked or undergarment-clad genitals, pubic area, buttocks, or

[97] Based on Section 4 of the New Zealand Harmful Digital Communications Act 2015.

female breasts which is made—

(A) from beneath or under an individual's clothing; or

(B) through an individual's outer clothing in circumstances where it is unreasonable to do so; and

(b) includes an intimate visual recording that is made and transmitted in real time without retention or storage in—

(i) a physical form; or

(ii) an electronic form from which the recording is capable of being reproduced with or without the aid of any device or thing."

Recommendation

146. Presently, nothing in our laws prevents someone from consulting child pornographic websites. Therefore, the Commission proposes to add **a new Section 15A to the Child Protection Act**[98], entitled ***Usual consultation of child pornographic sites***, which would read as follows:

> *"The fact of consulting habitually or in return for a payment a public online communication service providing an image or representation of a minor of a pornographic nature, to acquire or stock such image or representation by any means whatsoever shall be punished by imprisonment for a term not exceeding two years and a fine not exceeding 10 000 rupees."*

This new Section **criminalizes the usual consultation of child pornographic sites**. When the consultation is done in return of a payment, it does not have to be "habitual" and just one consultation would be enough for the offence to be constituted.

Those who set up websites showing child pornography shall fall either under the new Section 251 of the Criminal Code concerning "Debauching youth" or under 46 (ga) and Section 46 (h) (i) of the ICTA, as those two provisions use the terms "show a message" and "transmission (…) of a message" respectively, and which would be "abusive" in the first place and "greatly offensive" in the second, which is the case for child pornography.

[98] Based on article 227-23, al. 4 of the French Penal Code.

COURT ORDERS

Recommendation

147. The Commission is in favour of amendments to the ICTA so as to **introduce new Sections 46A[99] and 46B[100]** which would read as follows:

"***46A Restraining Orders***

(1) Where a person is guilty of an offence under Section 46, subsection (g), (ga) and (h) of this Act, the court may, ***in addition to or as an alternative to any other penalty****, order that the person* ***shall not, for such period as the court may specify, communicate by any means with the other person or that the person shall not approach within such distance*** *as the court shall specify of the place of residence or employment of the other person.*

(2) If on the evidence the court is ***not satisfied that the person should be convicted of an offence under Section 46 subsections (g), (ga) and (h) of this Act, the court may nevertheless make an order under subsection (1)*** *upon an application to it in that behalf if, having regard to the evidence, the court is satisfied that it is in the interests of justice so to do.*"

[99] Based on Section 10 of the Ireland Non-Fatal Offences Against the Person Act 1997.
[100] Based on Section 19 of the New Zealand Harmful Digital Communications Act.

46B Other Orders that may be made by the Court

The Court may, on an application, make 1 or more of the following orders against a defendant ***found guilty of an offence under Section 46 subsections (g), (ga) and (h)****:*

(a) an order to take down or disable material:

(b) an order that the defendant cease or refrain from the conduct concerned:

(c) an order that the defendant not encourage any other persons to engage in similar communications towards the affected individual:

(d) an order that a correction be published:

(e) an order that a right of reply be given to the affected individual:

(f) an order that an apology be published."

148. This would ensure that the victim can gain relief in cases where imprisonment may not be appropriate.

JURISDICTIONAL ISSUES AND HARMFUL COMMUNICATIONS

149. It is recommended, as was proposed by the Law Reform Commission of Ireland, that extraterritorial effect should apply to harmful communication offences.

Recommendation

150. In the Interim Report on Reform of the Criminal Code (May 2016), it was proposed to include a **new Section 3B entitled "Territorial applicability of criminal law"**.[101]

According to Subsection (5), Mauritian criminal law is applicable to any person who, within the territory of the Republic of Mauritius, is guilty as an accomplice to a crime or misdemeanour committed abroad if the crime or misdemeanour is punishable both by Mauritian law and the foreign law, and if it was established by a final decision of the foreign court.

Subsection (6) provides that Mauritian criminal law is applicable to any crime committed by a Mauritian national outside the territory of the Republic of Mauritius.

Moreover, according to Subsection (7), Mauritian criminal law is applicable to any crime, as well as to any misdemeanour punished by imprisonment, committed by a Mauritian or foreign national outside the territory of the Republic of Mauritius, where the victim is a Mauritian national at the time the offence took place.

[101] Based on articles 113-1 à 113-13 of the French Penal Code.

151. Thus, we see that the new provisions which are being proposed would cater for many harmful communications offences which are committed abroad.

CONCLUDING OBSERVATIONS

152. Our lives have been transformed by digital technology and this has created a "digital safety gap" which is being exploited by criminals. Indeed, between fake profiles, fake news, hate speech or online harassment, one can hardly say that digital communications and in particular social media are a safe place to navigate.

153. This is why many countries have embarked on a reform of their laws pertaining to harmful communications and digital safety. Basing ourselves mainly on the recommendations by the Law Commissions of Ireland and New Zealand, but also on reforms undertaken in countries like the UK, Germany, France, or Malaysia, the Law Reform Commission has come up with some proposals to strengthen our legislation in relation to that subject.

154. It has been observed by many commentators that specific laws intended to combat fake news could have a detrimental effect on freedom of expression, this is why the Commission is not favourable to enacting such a piece of legislation.

155. In other areas, however, like identity theft and fake profiles, grooming, stalking and court orders, the Commission has proposed the introduction of new provisions in view to combat this new kind of offence. It has also been suggested many amendments to existing provisions to more effectively curb online harassment.