Journal of Rights and Justice

2024/2025 – Vol 4

Journal of the Centre for Rights and Justice, Nottingham Law School, Nottingham Trent University

Journal of rights and justice-ISSN 2732-4265

EDITORIAL – Rev'd Prof Helen Hall

This latest edition of the *Journal of Rights and Justice* has maintained the standards set by the previous volumes, again presenting a diversity of topics and depth of exploration of the issues raised. On this occasion we open with an article from Maria Lyons on "Institutional child sexual abuse: an analysis of the response of the Roman Catholic Church and the state and its effect on the protection of children." In a world where such revelations of endemic abuse continue to arise from the voluntary and faith sectors, scholarship in this area remains much needed.

We then move on to the very different realm of data protection, with Alex Garment's thoughtful reflection on "A comparison of Hong Kong's PDPO and the European Union's GDPR in the context of the United Kingdom's DPA 2018". Finally, remaining with legal and social problems connected with navigating an increasingly digital world, we tackle the challenges of regulating AI with and an insightful offering from Sid Ali Boutellis "AI tipping point: an analysis of the EU & China's regulatory approach"

As always, the journal is dependent upon the hard work, professionalism and dedication of the editorial team. My heartfelt thanks go to Dr. Ryan Cushley-Spendiff for his energy and attention to detail as Deputy Editor, and for the invaluable administrative support of Kerri Gilbert. I am grateful as always to Prof Tom Lewis (Director of the Centre for Rights and Justice) and Prof Jonathan Doak (Associate Dean for Research, Nottingham Law School) for their wise advice and encouragement. Finally, although they must, for obvious reasons remain anonymous, I am hugely appreciative of the colleagues who have given their time and skill to undertake peer reviews, as without them, the journal could not exist in its present form.

	CONTENTS	
	Editorial	2
MARIA LYONS	Institutional child sexual abuse: an analysis of the response of the Roman Catholic Church and the state and its effect on the protection of children	5
ALEXANDER J.D GARMENT	A comparison of Hong Kong's PDPO and the European Union's GDPR in the context of the United Kingdom's DPA 2018	38
SID ALI BOUTELLIS	AI tipping point: an analysis of the EU & China's regulatory approach	63

INSTITUTIONAL CHILD SEXUAL ABUSE: AN ANALYSIS OF THE RESPONSE OF THE ROMAN CATHOLIC CHURCH AND THE STATE AND ITS EFFECT ON THE PROTECTION OF CHILDREN

*MARIA LYONS**

1. INTRODUCTION

Decades of institutional child sexual abuse necessitates analysis of environments that perpetuate such abuse.[1] Full disclosure and understanding of instances of child sexual abuse is crucial to effectuate corrective action and develop child protection strategies to prevent future abuses of power. This article aims to examine the response of the Roman Catholic Church (hereafter referred to as 'the Church') and the State to child abuse allegations in England and Wales. For the scope of this discussion, child abuse is a form of maltreatment of a child by inflicting harm or failing to prevent harm.[2] Child sexual abuse is a form of child abuse that involves forcing or enticing a minor to take part in sexual activity.[3] This can involve physical contact including assault by penetration such as rape, or non-penetrative acts such as masturbation and touching.[4] It can also involve non-contact activities involving grooming a child in preparation for abuse.[5] In England and Wales, sexual activity with a child is a criminal offence under the *Sexual Offences Act 2003*. In England, a child is defined as anyone who has not yet reached their 18th birthday.[6] Similarly, in Wales, a child is defined as 'a person who is aged under 18'.[7] However, it should be noted that the fact that a child has reached age 16 and can legally consent to sexual activity and live independently does not change their status of entitlement to protection.[8] For instance Neil Todd, who was 17 when the abuse suffered by Church of England Bishop Peter Ball began, was still entitled to protection.[9] Ball was convicted in 2015 and sentenced to 32 months in prison for sexual misconduct in relation to children under 18, despite Todd already reaching the legal age of consent when the abuse started.[10]

Child sexual abuse is particularly prevalent in institutions as they are in a unique position due to the culture and dynamics of power in institutional settings.[11] In the 2019 Crime Survey for England and Wales, the abuse suffered by 9.7% of adults who had been sexually abused in childhood had been carried out by a 'person in a position of trust or authority' such as a teacher, doctor, carer or youth worker.[12] This shows that clerical child sexual abuse is part of a wider issue that must be addressed. The Church as an institutional environment occasioning child sexual abuse however is particularly noteworthy due to its significant influence and power over children and their families. Although that is not to say that child sexual abuse is not an issue amongst other religious denominations and faith groups. This article will focus on the Roman Catholic Church, principally due to its global and unique management structure that has enabled large-scale cover-up and secrecy resulting in wholesale failure to protect children.[13] The large centralised organisational system of the Catholic Church has led to more media coverage and investigations compared to other religious denominations, such as Protestant churches which have independent smaller structures of various denominations.[14] This gives the Church a more global status as the organisation tends to be viewed as a whole, which is why issues concerning the Church in different countries are often interlinked as similar structures and practices are used. The scope of this article is therefore focused on the Roman Catholic Church, taking into account its global status and influence on the child sexual abuse crisis worldwide. In 2014, the Church's children's rights record was reviewed by the United Nations for the first time in almost 20 years.[15] Whilst the report focused on the Catholic Church and Catholic institutions, it duly recognised that 'other churches and religious institutions are also implicated in historic and current sexual and physical abuse of children'.[16] The report was aimed as a starting point to ultimately further expand their research and understanding of clerical child abuse, as it began to consider the fundamental issues with the Church.[17] This article will similarly focus on the Roman

Catholic Church as an institution which has been subject to intense media coverage and investigation due to its fundamental status and influence on the trajectory of the child sexual abuse crisis.

The article aims to examine the response of the Church after the abuse has occurred and how the criminal justice system continues to fail victim-survivors. Three main elements of this response will be discussed. Firstly, the safeguarding legislative framework will be examined to determine how child protection is regulated and implemented in the Church. More importantly, it will be argued that the absence of a unified approach and lack of full implementation have failed to protect children in accordance with this framework. Secondly, there have been a number of inquiries to investigate the extent and scope of child sexual abuse in the Church. The Nolan Report will be considered in light of its attempt to create a unified approach across individual dioceses, as well as the Cumberlege Commission's criticisms of the Report. Thirdly, the UK government's response to child sexual abuse will be considered in the context of 'position of trust' provisions. This will be demonstrated as the main reason as to why perpetrators escape prosecution. It will ultimately be argued that law reform is necessary to widen the scope of the legal definition, as well as raising awareness of the meaning of such provisions in Church environments and beyond.

The article will proceed to consider global perspectives. Whilst clerical child sexual abuse is an endemic issue[18], the discussion will centre on three jurisdictions due to their impact on understanding of child sexual abuse and criminal justice. Firstly, the USA will be considered as the birthplace of the child sexual abuse 'crisis'. Secondly, the Republic of Ireland will be considered due to the Church's unique relationship with the State that perpetuates child sexual abuse. Thirdly, Australia's response will be considered as its inquiry is considered as having the largest global impact. Particular attention will be drawn to legal developments in Victoria and

New South Wales in the form of criminal law duties to hold perpetrators and church leaders who failed to disclose abuse accountable, as well as the significance of mandatory reporting. The article will conclude with a short discussion on the Pope Francis' response to the child sexual abuse crisis and whether actions align with promises.

2. SAFEGUARDING FRAMEWORK

2.1 Safeguarding and Child Protection Legislation

Safeguarding is the action taken to promote the welfare of children and protect them from harm.[19] Child protection is part of the safeguarding process. It focuses on protecting individual children identified as suffering or likely to suffer significant harm.[20] This includes procedures which detail how to respond to concerns about a child.[21] England, Wales, Scotland and Northern Ireland each have their own framework of legislation, guidance and practice to identify children who are at risk of harm, take action to protect those children and prevent further abuse occurring. Laws are therefore passed to prevent behaviour that can harm children or require action to protect children, with guidance setting out what organisations should do to keep children safe.[22]

Safeguarding and child protection guidance places a duty on organisations to promote children's welfare and protect them from harm. Elliott argues that 'safeguarding the vulnerable child within the Church is of critical and fundamental importance not only to the child, but to the institution itself'.[23] Faith can play a major role in the lives and development of young people, and the Church should be a safe organisational environment for children. However, clerics, church leaders and children instructors who are to protect children are often the ones breaching such safeguarding principles.[24] Before considering the failures to protect vulnerable children in the Church, it is necessary to consider the safeguarding framework and development of the law relating to children in England and Wales.

There is no single piece of legislation or guidance that deals with all aspects of child welfare and safeguarding in the UK which leads to inconsistent implementation. There are a number of different laws and regulations relating to different bodies which are frequently subject to amendment and change. In the context of child abuse, *Working Together for the Protection of Children Guidance 1986* [25] was issued to local authorities, police forces and voluntary organisations which set out agencies' responsibilities and procedures for working together. The Child Sexual Abuse chapter was frequently updated to take account of more recent legislation, such as the *Children Act 2004*[26] and *Education (Independent School Standards) Regulations 2014*.[27] These amendments indicate how there is no single, formal guidance or strict rules that local authorities and organisations must follow. This creates difficulty when the safety and wellbeing of vulnerable children comes into question as there is no single framework to standardise actions across organisations.

Regarding the protection of children, it is important to consider the *Children Act 1989*. This gave every child the right to protection from abuse and established key principles which govern the way decisions concerning welfare and safety of children are made. In particular, when a court determines any question with respect to the upbringing of a child, administration of property or application of income, the child's welfare shall be the court's paramount consideration.[28] This is known as the paramountcy principle, meaning the child's best interests are the court's sole concern. The importance that the law affords to such a consideration can be evidenced by the House of Lords decision in *J v C (An Infant)* which clarified interpretation of 'paramount'. [29] Lord McDermott explained that 'when all the relevant facts…are taken into account and weighed, the course to be followed will be that which is most in the interests of the child'. [30] This approach has been consistently favoured, being re-affirmed in *Re W (A Child)*

(Adoption: Delay) where it was held that the interests of the child 'takes precedence over the claims and rights of even the most unimpeachable parent'.[31] This makes clear the primary importance with which the law treats the welfare of the child through legislation, guidance and case law. However, as will be demonstrated, institutions often fail to treat the rights and interests of children with such importance.

The rationale behind the introduction of child protection legislation and guidance was to provide a framework for the safeguarding of children in England and Wales.[32] It imposed a duty on local authorities to safeguard and promote the welfare of children in need.[33] It is clear that these provisions were intended to create institutional environments that focussed primarily on the welfare and safeguarding of children which is indicated by the mandatory nature of the 'duties' imposed on institutions.

2.2 A Programme for Action (The Nolan Report)

These welfare considerations have not always been followed in practice. In an attempt to provide a code of practice for safeguarding and welfare of children, the Home Office's '*Safe from Harm'* laid out thirteen core principles that voluntary organisations should consider.[34] In 2001, the Nolan Report recommended that the Church adopt these guiding principles to create a safe environment for children.[35] The purpose of the report was twofold; to examine and review arrangements made for child protection and prevention of abuse within the Church and to make recommendations to implement such protection measures.[36] As there was no single piece of guidance or rules for churches to implement child protection measures, the report intended to create a unified Church-wide commitment to child protection based on the paramountcy principle.[37]

However, although creating a cohesive approach is desirable to regulate institutional environments to consistently uphold the paramountcy principle, a single set of policies presents difficulty in practice. This is due to the complicated structure of the Church which is made up of dioceses and religious orders. A diocese is a 'district under the pastoral care of a bishop' in the Christian Church.[38] A religious order is 'a group of men and women living a common life bound by vows under an officially approved rule of life'.[39] These religious orders are governed by their own law and constitutions. In general, diocesan bishops have no capacity to intervene in their internal affairs. Despite this concern, making recommendations and arrangements for child protection was intended to emphasise that formal responsibility for action lies primarily with individual bishops and superiors of religious orders.[40] However, this is a challenging starting point as there is no clear line of accountability due to the ad hoc structure of the Church which allows individuals to hide behind religious superiors and makes individual responsibility unlikely.

The Nolan Report led to the establishment of the *Catholic Office for the Protection of Children and Vulnerable Adults*.[41] Chair of the independent management board, Archbishop Nichols, wrote that Nolan's recommendations were 'accepted' and that the work 'represents a sea-change in many of the habits and procedures that underlie the life of the Church'.[42] However, I argue that describing the work implemented as a 'sea-change' is an overstatement. Although it was recommended that Child Protection Co-ordinators and Representatives should be informed of every disclosure of abuse and common practice should be established, individual monasteries and abbots were left to decide whether and to what extent to implement these recommendations.[43] For example, Ampleforth was one of two abbeys that chose instead to set up its own internal safeguarding commission rather than align itself with the diocesan safeguarding commission.[44] This undermines the aim of creating a unified approach as the approaches adopted by individual religious orders would be inconsistent. Further, Gilligan noted several failures of the Church to respond to the recommendations, namely failure to consistently

laicize perpetrators, as well as survivors continuing to have negative interactions with Church leaders in response to their abuse.[45] In 2014, 52 priests had been laicized since the recommendations in 2001.[46] This is irreconcilable with the 456 sexual assault claims made against clergy members between 2003 and 2012.[47]

2.3 The Cumberlege Commission

In light of the recommendations made in 2001, the Cumberlege Commission conducted a critical review of child safeguarding structures and published its report entitled 'Safeguarding with Confidence'.[48] This report identified a number of misgivings with the Nolan Report. Firstly, it assumed the Church operated as a functioning, hierarchical organisation capable of responding to and implementing a secular model of child protection.[49] The reality however is different. The Catholic Church is collegiate, not a homogenous organisation with lines of accountability as generally understood by the secular world.[50] As the Church is made up of dioceses and religious orders, authority rests with each Bishop in his diocese and each Congregational leader who have differing priorities and levels of resources.

Secondly, priests have been resistant to change due to fear and suspicion that the authority of leadership is being undermined. This impeded delivery of effective safeguarding arrangements and the paramountcy principle has not been upheld. An Australian inquiry into child abuse in religious organisations found that many religions operate under an internal legal system of religious laws.[51] In the Church, this is the 'Code of Canon Law'[52] which is defined as 'the law governing the affairs of the Christian Church, especially the law created or recognised by papal authority in the Roman Catholic Church'.[53] Canon law has authority only for that Church and its members.[54] In practice, religious officials use these 'confusing and self-serving laws to usurp the role of secular law enforcement'[55] as members of the Church view its Canon law as a means by which they are excluded or exempt from local laws. This is equally applicable in the

context of England and Wales as the acts of religious leaders reflect the attitude of being above secular law. There are fundamental differences in the ways that Canon law and secular law approach child sexual abuse cases. Canon law views punishment as a 'last resort'[56] as 'the salvation of souls…must always be the supreme law in the Church'.[57] By contrast, in secular criminal law, justice demands 'that an appropriate punishment is given'.[58] Accordingly, a person found guilty of sexual activity with a child is liable, on conviction on indictment, to imprisonment for a term not exceeding 14 years.[59] For instance, the Ampleforth and Downside Investigation Report, which concerned leading Catholic independent schools, emphasised that the overriding concern of religious leaders was not to refer the suspected perpetrator to the police for appropriate punishment.[60] Rather, religious actors aimed to avoid contact with local authorities and police at all costs in favour of rehabilitation.[61] For example, following parents' complaints that Father Piers Grant-Ferris had inappropriately touched their son, an internal investigation was conducted. Consistent with the commitment to 'salvation of souls', he was assessed by a consultant psychiatrist as they aimed to 'avoid the spread out of the sphere of the ecclesiastical authorities' and 'to prevent involvement of statutory authorities'.[62] This view reflects the attitude that Canon law should prevail, thus justifying their attempt to engage in psychological rehabilitation rather than reporting the crime to the police.

Consequently, clergy members feel that their unique authority is threatened by such recommendations as contained in the Nolan report; the view largely to blame for the significant failures to protect children. The investigation rightfully outlines that this legal structure creates a complication unique to religious organisations that operate under a separate system to secular society, ultimately leading to an 'additional layer of coverup to be penetrated and removed to protect children'.[63] Use of these religious laws enables members of the Church to hide the truth, protect dangerous predators and continue to silence victims. White and Terry argue that Canon Law's purpose is to promote Christian living rather than provide justice as the criminal justice

system does.[64] This perceived authority that usurps secular accountability creates a shield for perpetrators to hide behind, thus it is unsurprising that Church members were reluctant to respond unequivocally to recommendations.

Thirdly, clerical attitudes towards safeguarding have largely hindered the aim of protecting vulnerable children. Cozzans blamed ecclesiastical authorities for prioritising the institutional welfare before the safety of its most vulnerable members.[65] Similarly, Robinson blamed clerical authorities for promulgating and maintaining silence over the whole issue.[66] Rashid et al go further to emphasise that these clerical tensions nurtured the gap between clergy and their respective Bishop and Congregation leader, leading to an erosion of trust and creating fear of a malicious allegation.[67] This absence of will by the members of the institution is a significant impediment to achieving justice for survivors of child sexual abuse because as long as attitudes continue to overlook the issue, the less likely substantial change is to be seen. Due to discretion afforded to church leaders in implementing protection measures, this structure places those who embody such attitudes into sole power which substantially impedes corrective action in how the Church deals with abuse. It can therefore be argued that the Nolan Report simply perpetuated the power afforded to Church leaders and a stricter approach was needed to ensure recommendations were unequivocally adopted.

Academic commentary is conflicted as to which approach is most appropriate for the Church. Gula insisted upon development of a 'Catholic Code of Ethics' that clearly defined the primary values and moral obligations, professional responsibilities and development of professional procedures to regularly evaluate ministerial performance.[68] In contrast, Coquillette and McMorrow argued that no code of ethics could prevent intentional wrongdoing in violation of criminal law as the former is directed at individual misconduct and thus could prove ineffective

for suitable changes in institutional structures.[69] Rashid et al support the latter view, arguing that 'no ethical approach could avert intentional wrongdoing but appropriate accountability mechanisms and management policies' would better tackle abuse behaviours.[70] These views are convincing insofar as perpetrators must be held accountable and management policies can help create a culture of vigilance towards child sexual abuse allegations. Arguably however, in England and Wales, the most pressing area which requires response is criminalising such behaviours. Criminalisation is the most serious method by which the law in England and Wales can condemn certain acts. Rape, assault, assault by penetration and causing or inciting a child to engage in sexual activity and other specific child sex offences are criminal offences under the *Sexual Offences Act (SOA) 2003*.[71] This indicates the seriousness of such offences which should apply equally to clergy as it does the laity. However, clergy members often escape prosecution due to position of trust provisions that are narrowly defined.

3. POSITION OF TRUST

3.1 Loophole in the law

There are significant failures in the secular legal system that enable perpetrators to cover up child sexual abuse and escape prosecution. The 'position of trust' provision in the *SOA 2003* has been described as a 'loophole' in the current law. Under *ss16-19*, it is unlawful for someone in a position of trust to engage in sexual activity with a child in their care aged 16 or 17 years old. This was intended to protect those who are above the age of consent but still vulnerable to abuse and exploitation in institutional contexts. This is clarified as a person who is 'regularly involved in caring for, training or supervising'[72] and 'regularly has unsupervised contact'[73] with a young person. However, the law narrowly defines specific roles and settings where sexual activity between an adult in a position of trust and a young person is illegal. The definition only applies to adults working in a set of professions listed in *s21* of the Act, including teachers, care workers

and youth justice staff. However, the definition does not include religious leaders. Sarah Champion MP argues that these leaders clearly meet the criteria due to their regular unsupervised involvement with children but are absent from the list of professions, allowing them to be above the law and engage in sexual activity with 16 or 17 year olds in their care 'with impunity.'[74] Government inaction to include religious leaders in the legal definition simply allows the adult in a position of trust to argue that a young person consented to the sexual activity. Faith leaders should be captured under this definition due to their regular and close contact with young people and their families who place significant trust in them.

3.2 Law Reform

Law reform is needed to expand the legal definition in order to hold more perpetrators accountable for abusing their power by exploiting vulnerable children in the Church. Proposals for reform were largely driven by 'thirtyone:eight'[75] who published a report which deals with closing the gap in the law and points out the inconsistency between the *SOA 2003* and *Safeguarding Vulnerable Groups Act (SVGA) 2006*. The *SVGA 2006* contains provisions on 'regulated activity and enhanced criminal records disclosures which define position of trust in a wider and more inclusive way'.[76] This is not consistent with the current narrow law on sexual offences which illuminates the UK government's failure to align child protection and sexual offence legislation. This leads to a lack of legal certainty and understanding of the provisions as young people are still vulnerable to abuse, thus undermining the paramountcy principle. This inconsistency has been noted and targeted in other jurisdictions. The law in Australia was amended to include religious leaders in the State of Victoria. The *Crimes Act 1958* was amended in 2016 to include 'a religious or spiritual guide, or a leader or official of a church or religious body'.[77] Therefore, children in the UK would potentially receive more effective justice if the legal

definition of position of trust was widened to ensure a wider range of perpetrators are covered and unable to escape prosecution.

However, the Parliamentary Under-Secretary of State for Justice, Alex Chalk, expressed concerns of widening the legal definition due to the danger of infringing upon the autonomy of 16- and 17-year olds who are considered consenting adults under UK law.[78] Chalk argued that any broad new definition could raise the age of consent by stealth.[79] The law in the UK acknowledges that children have a right to autonomy as evidenced by the age of consent, as well as the right to private and family life under *Article 8* of the *European Convention on Human Rights*.[80] However, the law must 'not create an imbalance or inconsistency in robustness of how young people and children are afforded the right to protection from harm and abuse, resulting in a postcode lottery based upon setting and role.'[81] It is therefore vital that the law responds to this loophole to prevent fundamental failures to protect children in line with the paramountcy principle and provide justice for victims who have not been protected by the Church. It is indeed true that a balance needs to be struck between rights of consenting individuals and protecting children, however the latter consideration cannot merely be overlooked and must be amended to prevent clergy members escaping prosecution.

In response to campaigns and parliamentary lobbying, the *Police, Crime, Sentencing and Courts Bill 2021* aims to amend the *SOA 2003* to extend position of trust offences under *s22A* to include certain activities in a sport or religion.[82] At the time of writing, the Bill is not yet finalised, thus it is too early to understand whether changes to the provisions will result in more prosecutions of religious leaders abusing their position of trust. However, it is likely that amendments to the law will not be enough in itself to ensure future cases are prosecuted. The 'thirtyone:eight' report proposes that the government launch a public campaign to communicate the change in legal definition so adults working with children are aware that it is illegal for any

adult to engage in sexual activity with a child under their care.[83] This replaces any opportunity that adults in a position of trust have to escape and exploit the definition under current law with a clear message that it is illegal to have sexual activity with a 16 or 17-year-old under their responsibility. It is also proposed that the government 'work closely with faith, sports and safeguarding organisations to ensure messages are clear and consistent'.[84] This would aid the government in aligning the law with safeguarding provisions and rightfully place vulnerable young people's safety at the forefront of organisations that assume responsibility for such individuals. However, whether this occurs depends on the extent to which faith-based organisations commit to and adopt the legal changes by creating a culture of transparency and full disclosure when sexual abuse allegations are reported, which will enable such cases to be fully investigated and prosecuted accordingly. Nevertheless, law reform relating to position of trust is long overdue.

4. GLOBAL PERSPECTIVES

4.1 USA

Following widespread media attention, the case of Father Gilbert Gauthe in 1983 who had raped and sodomised young boys and used his authority as a priest to 'intimidate them into silence' was a catalyst for clerical child sexual abuse being viewed as a 'crisis'.[85] The response of the Church, namely apologising for sin, sending the perpetrator for psychological evaluation or treatment, and moving the priest to a new parish or school,[86] enabled a cycle of abuse where perpetrators were not held accountable.

In 1992, the United States Conference for Catholic Bishops (USCCB) established the 'Five Principles' to create transparency when dealing with allegations.[87] In particular, they urged laicising the alleged offender if there is sufficient evidence and cooperation with the investigation.[88] Although the USCCB argued that many dioceses implemented these principles,[89] Frawley-O'Dea doubts whether

this was the case. She argues that execution of these principles depended on the individual bishop's determination that there was sufficient evidence to support an allegation, which in turn led to many bishops 'unable or unwilling to discern the credibility of an accusation'.[90] It is logical that the principle of collecting sufficient evidence would be ineffective at the outset as evidence should be gathered at the investigative stage by authorities rather than by clergy. This further represents the failure to treat child sexual abuse as a criminal act in favour of viewing the crisis through the lens of sin and forgiveness. Similar to the approach in England and Wales, large discretion afforded to clergy members enables them to consistently coverup allegations.

Furthermore, Terry highlights that few priests accused of sexual abuse were arrested or processed through the criminal justice system.[91] As well as bishops helping abusers through psychological support and treatment, there was a substantial delay in the reporting of most offences which was often after the statute of limitations expired.[92] Abuse is widespread but underreported as victims are often discouraged from reporting due to fear of not being believed and having to recall details of the abuse which is especially traumatising for children. For example, the Crime Survey for England and Wales recently estimated that of 3.1 million adults aged 18-74 who experienced sexual abuse before the age of 16, only 30.2% reported it to someone in an official position.[93] The Office for National Statistics highlights that understanding how many victims do come forward is important to know the resources needed to support the child protection system as victims of child sexual abuse often remain hidden.[94] Naturally, this is exacerbated by the secrecy and cover up by the Church which further supresses children's traumatising encounters. A culture of transparency is needed within the Church, as well as encouraging victims to come forward and creating a safe space for children and adults in the criminal process to ensure survivors receive justice.

Clohessy argues that victims cannot promptly report such crimes, but 'need decades of recovery before being able to talk' with legal professionals.[95] Therefore, legislators in the USA enacted civil window laws which enable anyone who was abused by anyone in any institution to sue, usually for a year or two only, the wrongdoers who committed and concealed child sex crimes.[96] It can be argued that statute of limitations are generally favourable as it can be difficult for judges and juries to confidently make judgements if witnesses forget and evidence is lost over time. However, Clohessy helpfully draws a distinction between victims to a crime more generally, who may be encouraged to come forward earlier, and child sexual abuse victims who 'face powerful psychological barriers that make recognizing and disclosing the crimes and damage exceptionally tough.'[97] He also proposes that Catholics should spread the word about these legal opportunities for victims, including parishioners.[98] In line with creating more transparency and disclosure, this is an essential action for the Church to take if it is to become proactive and protective of vulnerable children.

Similarly, in the civil law context in England and Wales, all claimants have until at least the age of 21 to commence legal proceedings as it is recognised that 'very few victims and survivors of child sexual abuse bring their claims before the age of 21'.[99] As a result, victims and survivors can invoke s33 of the Limitation Act 1980 to ask the court to exercise its discretion and allow them to proceed with their claim despite being past the limitation period.[100] This permits the court to take into account such factors as the reasons for delay in bringing the claim.[101] This affords the court discretion to consider how traumatising and difficult it can be for survivors to come forward. Affording survivors such opportunities in the civil legal processes in the USA and England and Wales are vital to ensure the State's commitment to facilitating protection of those who suffered abuse in childhood which is understood to be highly traumatising and potentially

damaging. This puts the needs of children and adults at the forefront of the civil justice process and is essential to ensure that sexual abuse victims are not left behind.

4.2 Ireland

Since 2000, reports began to consistently emerge about abuse in other countries which gave the impression that child sexual abuse was an endemic crisis.[102] Ireland is viewed as one of the most Catholic countries in the world as Catholicism is deeply rooted in Irish politics and has a particular privilege due to its close association with Irish nationalism and resistance to British rule. This contributes to the influence the Church can have over the law and the 'trust and respect placed by Irish society in its clergy'.[103] It should be noted that Ireland operates within a separatist system. The Irish Constitution provides for Church-State separation through the endowment clause which guarantees that the State 'does not endow any religion'.[104] Despite this apparent separation, the influence of the Church and Christian is evident in Irish case law. For example, in *Norris v Attorney General*, O'Higgins CJ emphasised that 'a deep religious conviction and faith and an intention to adopt a Constitution consistent with that conviction and faith and with Christian beliefs' are enshrined in the Preamble.[105] This suggests that the courts have interpreted the Constitution in the context of Christian beliefs, emphasising its established role in Irish law and society despite its theoretical separation.

Ireland's first case of public attention was Father Brendan Smyth who sexually abused 140 children over 4 decades.[106] Fr Smyth faced no repercussions[107] and went on to continually sexually abuse children for a further 19 years.[108] Pang, Hogan and Andrasevic argue that this case denotes how the Church prioritised the protection of its reputation over child welfare.[109] This is further supported by McAlinden who links the case with Taoiseach Albert Reynolds' resignation[110] following revelations that the Attorney General delayed Smyth's extradition.[111] The Taoiseach's resignation reflects the inextricable link between the Church and State as the Head of State is

influenced not only by political and public opinion but the actions of the Church, further reiterating the hegemony of the Church which has influence on politics and law making. Whilst the Supreme Court has generally created a 'wall of separation' between the Church and State in the US[112], this relationship in Ireland is vague and flexible. Indeed, Hogan highlights 'the pernicious nature of the symbiotic relationship of church and state that allowed the abuse to go unchecked'.[113] Although the Church and the State are fundamentally and constitutionally separate, the Church's undeniable influence creates another barrier to truth commission and justice for victims of sexual abuse as the Church can effectively hide behind their cultural and political indemnity.

Following a number of reports published by the *Commission to Inquire into Child Sexual Abuse*[114], a significant development was its report into the Archdiocese of Cloyne in 2011 as it is only the immediate aftermath of this report that proposals for significant reform came to fruition.[115] The *Criminal Justice (Withholding of Information on Offences Against Children and Vulnerable Persons) Act 2012*[116] criminalises failure to disclose important information about potential abusers. This is based on knowledge or belief that an offence has been committed against a child which should be disclosed to the Garda Síochána.[117] The *Children First Act 2015* also places statutory obligations on groups of professionals and particular organisations to report reasonable belief or suspicion that a child is being or has been harmed.[118] Although the Act mandates professional individuals who are working with children to report concerns, Bourke and Mounsell note that the legislation does not provide sanctions for mandated reporters who fail to comply with the Act.[119] However, individuals such as teachers 'do not feel that they are adequately trained' to report suspicions of abuse.[120] This conclusion may change in light of the *Children First National Guidance in 2017* which provides that Tulsa, the Child and Family Agency, can take administrative actions if it emerges that a professional did not make a mandated report and a child was significantly harmed.[121] Additionally, Tulsa's 'Protocol for Mandated Assisting' to

support and reinforce the practice may reduce pressure on professionals who have more guidance and understanding of how and when to report.[122] However, despite the benefit of hindsight informing Bourke and Mounsell's conclusion, it is likely that holding professionals legally accountable for failing to report is to be more effective in line with the statutory offences already contained in the *Criminal Justice Act 2012*.

McAlinden contrasts the legislative approach in Ireland with England and Wales where legislative action is seemingly more readily taken. For example, the *Safeguarding Vulnerable Groups Act 2006* was enacted to give effect to recommendations to the Bichard Inquiry in 2004[123] which examined the effectiveness of police responding to the murders of Jessica Chapman and Holly Wells.[124] In contrast, despite the number of inquiries from the early 2000s in Ireland, it wasn't until the *2012 Act* that major legislative change was made to respond to failures to implement recommendations to protect vulnerable children. Further, specific legislation targeting child sexual abuse wasn't enacted until 2014 with the *Safeguarding Vulnerable Persons at Risk of Abuse National Policy and Procedures*.[125] Delay in adopting a vigorous reformative agenda in Ireland is likely due to the intricate relationship between the Church and the State and tension between institutional failings and willingness of the institution to effect proposed changes.

4.3 Australia

The response of Australia to institutional child sexual abuse is particularly noteworthy as the Australian Royal Commission into Institutional Responses to Child Sexual Abuse (the Royal Commission) has been described as 'one of the most important public inquiries into institutional child abuse globally.'[126] There have been a number of legal developments influenced by its findings, particularly legal duties with a strong focus on disclosure of known and suspected child abuse. In Victoria, an adult who has reasonable belief that a sexual offence has been committed

is required to 'disclose the information to a police officer'.[127] The seriousness of the offence is indicated by a maximum penalty of 3 years' imprisonment.[128] Similarly, in New South Wales, there is a general duty in criminal law requiring adults to report known offences that implicitly include child abuse. For example, *s316 Crimes Act 1900* requires a person who 'knows or believes that a serious indictable offence has been committed'[129] and has 'information which might be of material assistance' in the investigation to report to the police.[130] In 2018, this was used to convict the most senior clergy member worldwide ever prosecuted for this offence.[131] Philip Wilson, former Archbishop of Adelaide, was found guilty of failing to report to the police the repeated abuse of two altar boys by paedophile priest, James Fletcher, during the 1970s and was sentenced to two years' imprisonment. However, on appeal, the conviction was overturned by the District Court judge who found reasonable doubt as to whether the disclosure was made and whether Wilson believed the disclosure if it was made.[132] Foley highlights how the acquittal suggests that the requirements under *s316* were 'extremely difficult' to establish.[133] Judge Ellis made clear that the Crown's assertion that Wilson 'must have' remembered being told of the abuse 'can never equate to proof beyond reasonable doubt'.[134] This indicates the high threshold for the prosecution to successfully discharge the burden of proof. This restricts the Crown's case and makes it exceptionally difficult to prove that the accused knew of the abuse. New South Wales have since introduced a specific charge to deal with failures to report child sexual abuse which makes 'concealing' such an offence indictable and up to 5 years' imprisonment.[135] Foley argues that the specific nature of this offence provides for a 'much more realistic credible threat'.[136]

Criminal law duties to report specific types of abuse co-exist with mandatory reporting legislation in many Australian states. This suggests a general commitment to mandatory reporting as a public policy to protect children from abuse. Despite challenges such as adequate resources needed to respond to demand for staffing and services, research has shown that more

cases of child sexual abuse are reported in jurisdictions which have enacted mandatory reporting legislation compared to those where the law does not exist.[137] This is supported by Matthews et al who found that mandated reporters of suspected child sexual abuse increased from 662 in the 2006-2008 pre-law period to 2,448 in the 2009-2012 post-law period.[138] The Welsh government has also introduced a legislative duty to report child abuse and neglect.[139]

However, it must be recognised that Australia has a different cultural and legal context, thus a system would need to be developed to accommodate mandatory reporting in the English framework. The ICCSA has suggested a mandatory reporting law which requires designated professionals who work with children to report cases they suspect.[140] For present purposes, such designated professionals in the proposed legislation include 'A minister of religion, religious leader or member of the clergy (however described) of a church or religious denomination'.[141] The proposed wording leaves identification of those who are subject to a duty to report open-ended through 'however described'. Although this could potentially be used to cover a broad range of clergy members who are responsible for children and by implication must report, difficulties in interpretation are likely to arise as to who exactly a 'member of the clergy' is. Further, this may not encompass other community members who undertake pastoral work and should be equally obliged to report any risk to the safety of a child that occurs in a religious setting.

Currently, the government in England has resisted mandatory reporting on the basis of complex difficulties as to who the duty falls onto and to whom they are to report. This is a legitimate concern as it is not entirely clear as to whom the duty attaches, which is particularly problematic for religious groups with different organisational structures. This is further exacerbated by recent developments in England and Wales in respect of tort law and vicarious liability. In the recent decision of *Trustees of the Barry Congregation of Jehovah's Witnesses v*

BXB, the claimant argued that the Jehovah's Witness organisation was vicariously liable for the rape committed by Mark Sewell, an elder from her local congregation of Jehovah's Witnesses, as they failed to take steps to protect her.[142] The UK Supreme Court (UKSC) considered the two stages to establish various liability. Despite agreeing with the lower courts that the relationship between Sewell and the Jehovah's Witness organisation was akin to employment, this relationship did not satisfy the close connection test due to a number of factors. For example, the rape was committed in his own home, not whilst carrying out activities as an elder,[143] and the UKSC was critical of the suggestion that he never took off his 'metaphorical uniform' as this was an 'unrealistic submission'.[144] Although the issue did not concern whether this person was a 'cleric', the parallel is evident. If such acts are not sufficiently closely connected to the exercise of his role, the mandatory duty to report may not attach to members of the Jehovah's Witness organisation in such circumstances despite the perpetrator's evident position of power. Although the claimant in the aforementioned case was an adult, the proposed legislation is likely to present difficulties in practice for future cases of institutional child sexual abuse due to the impact this narrow interpretation may have on who may be subject to a duty to report.

Indeed, the wording of mandatory reporting laws in Australia differs across states, suggesting lack of an all-encompassing definition. The wording of provisions in New South Wales and Victoria are vague and open-ended, subjecting 'a person in religious ministry, or a person providing religion-based activities to children' [145] and 'a person in religious ministry' [146] to mandatory reporting laws respectively. This vague wording potentially creates a wider spectrum of who may be considered subject to the duty. However, it equally creates considerable uncertainty as there is scope for argument that a person who failed to report is not captured under the definition due to lack of specific wording as to whom the duty attaches. In Australian Capital Territory, 'a minister of religion, religious leader or member of the clergy of a church or religious denomination' are mandated to report.[147] This is similar to the proposed legislation in

England and Wales in its attempt to cover a wider spectrum of those subject to a mandatory duty to report. Arguably, the wording of the proposed legislation is stronger than its Australian counterpart through the inclusion of 'however described'. This creates scope to argue that an individual is captured under the definition in relation to the particular religious organisation in question. That said, in light of recent developments in England and Wales, the issue remains that the lack of an all-encompassing definition and specific wording may result in many individuals, particularly lay persons, not being captured under the definition, thus limiting the effectiveness of mandatory reporting laws.

It is submitted that these issues may be overcome by placing a mandatory duty to report on those in a 'position of trust' as discussed previously. As its definition is in need of reform to create a broader spectrum of those considered to be in a position of trust, reform should be such that it encompasses different faiths and religious settings as well as members of the institution who are not responsible for ritual like priests. A position of trust is not specific to a particular religion or religious actor but should be interpreted as a person who has regular responsibility to care for, train or supervise a child. It has also been suggested earlier in this article that the government work closely with faith organisations to ensure the message and interpretation of such provisions are consistent. Therefore, incorporating the position of trust definition into mandatory reporting laws will create consistency and avoid confusion as the same definition is applied in respect of the threshold for criminal liability and the civil duty to report.

England is clearly behind its commonwealth counterparts in adopting mandatory reporting which has been proven to show a trend of a substantial increase in reports. As well as increasing awareness, it creates acceptable standards of behaviour and enables the government to monitor and evaluate trends of reporting in order to adequately inform child protection strategies and necessary systemic changes to protect vulnerable children. However, it is

recognised that implementation is not without its difficulties. Mandatory reporting laws must be developed carefully so as to encompass a variety of positions in organisations with different management structures.

The development of the legal system in Australia, particularly Victoria and New South Wales as the most populous states, demonstrates that legal intervention is required to protect vulnerable children who often cannot seek help. Matthews argues these developments respond to contemporary understandings of danger and the extent of institutionalised corruption.[148] This is clear through cases such as Wilson as the law was tightened by creating a specific offence for child abuse, meaning those who fail to report cannot escape prosecution as easily. This amendment was made in direct response to a significant judgment that was indicative of the law failing to protect vulnerable children and hold clergy members accountable. Matthews argues that although criminal law is generally concerned with prohibiting specific acts, duties may legitimately be imposed to criminalise omissions.[149] This is because children have a 'special vulnerability' and lack of power due to inherent physical and emotional vulnerability, as well as legal and economic dependence on adults.[150]

5. POPE FRANCIS' RESPONSE

Elected in 2013, Pope Francis called for decisive action in dealing with the ongoing child sexual abuse crisis.[151] The first concrete step to tackling the issue was the establishment of a child sex abuse commission to advise him on protecting children from paedophile priests and provide codes of conduct for Church officials in order to 'set a new tone in the governance of the church'[152] that had been called for by various inquiries and commissions globally. Furthermore, at an unprecedented summit on paedophilia in the Church, Pope Francis pledged to face every case with 'utmost seriousness' by reviewing and strengthening guidelines to prevent abuse and punish perpetrators.[153] Pope Francis changed the Church's laws to explicitly criminalise sexual

abuse which was the biggest overhaul of the criminal code for nearly 40 years.[154] Sexual abuse, grooming minors for sex, possessing child pornography and covering up abuse will be criminal offences under Vatican law. The new code replaces the previous outdated laws that were designed to protect perpetrators using clearer language that indicates the action that bishops must take when a complaint is made. However, the new laws do not spell out sexual offences against minors. They still refer to offences against the sixth commandment which prohibits adultery. The 2020 Report into child sexual abuse sponsored by the UK government states that 'describing child sexual abuse as the canonical crime of 'adultery' is wrong and minimises the criminal nature of abuse inflicted on child victims'.[155] As child sexual abuse is not explicitly framed as a criminal offence, this is inconsistent with Pope Francis' intention to explicitly criminalise such offences as the crime should be clearly defined as one against the child rather than a violation of priestly celibacy.

Pepinster argues that despite the Pope's efforts, 'reforms have got stuck' and the commission is no nearer to producing new ways of dealing with the issue.[156] This is evidenced by abuse victims who have resigned. Marie Collins, a survivor of clergy sexual abuse who serves on Pope Francis' Pontifical Commission for the Protection of Minors, resigned in 2017 due to the reluctance of members of the Vatican to implement recommendations.[157] Collins further criticises the use of 'adultery' in relation to sexual abuse of minors, arguing that it is 'inappropriate'.[158] The Church's argument that it is 'tradition' is reflective of its inability to respond to crisis circumstances and failure to explicitly take accountability for the crime of sexual abuse. Survivors on committees such as these are vital to progress the movement towards corrective action, although victims are being driven away due to the Pope's piecemeal reforms and failure to deliver on his promises of 'decisive action'. Laws which explicitly define child sexual abuse as understood by the secular world need to be incorporated in the Church's system of laws in order to ensure a vigilant and transparent handling of allegations.

6. CONCLUSION

This article aimed to analyse the response of the Roman Catholic Church to child sexual abuse allegations and identify where significant institutional failings lie. As such, an exploration of the safeguarding framework and child protection legislation was necessary to demonstrate the Church's failure to align child protection legislation and guidance with internal policies and practices. The absence of a single structured framework has significantly contributed to the culture of secrecy within the Church and its members, particularly due to lack of clear lines of accountability and vague provisions that are subject to frequent change. The basis for this conclusion was aptly exhibited by two investigations into clerical child sexual abuse. The Nolan Report theoretically established a commitment to a unified set of policies across dioceses and religious orders. However, in practice, this was a misguided approach as the discretion afforded to church leaders undermined the commitment to a unified approach and perpetuated the culture of secrecy and coverup. The Cumberlege Commission identified significant failings of the Nolan Report to enforce recommended policies in order to treat child sexual abuse with sufficient diligence. Three important interlinking reasons were identified. Firstly, it wrongly assumed that the Church operated as a homogenous organisation that could easily establish and implement the same policies. Initial recommendations were misaligned with the true structural nature of the Church that blurred lines of accountability through existence of multiple independent dioceses and religious orders. Naturally, implementation of recommendations was not consistent. Secondly, the Church's Code of Canon Law creates the impression amongst priests and religious leaders that they can usurp the authority of secular law due to different understandings of criminal justice. It should not be misunderstood that although subject to an internal system of laws, clerical perpetrators of child sexual abuse are committing a criminal act that should be prosecuted accordingly. Thirdly, and most damningly, attitudes towards child protection have substantially impeded adoption of safeguarding measures. This is largely due to

erroneous clerical attitudes that interpret unequivocal adoption of recommendations as a means of undermining the authority of the accused in favour of protecting the Church and its leaders.

As well as responses of the Church, the response of the State was considered in light of position of trust provisions under the *SOA 2003*. A stricter legal definition of position of trust is necessary to avoid perpetrators escaping prosecution as religious leaders are excluded from the legal definition. Although amendments are to be made, it is unclear whether the new provisions will result in more prosecutions and whether the provisions are understood by Church members. Accordingly, raising awareness and providing education to church members, professionals and parents on the meaning of such provisions is necessary in order to create legal certainty and transparency relating to church members' interaction with children in their care.

Comparative analysis of global responses demonstrated that the USA was the catalyst behind the growth of the endemic child sexual abuse crisis. The approach of Church leaders was to deflect attention from the crime itself towards retribution and support for the perpetrator in the form of psychological treatment, again viewing sexual abuse as a sin that could be forgiven rather than a criminal act. Significantly, church leaders were granted a great deal of power and authority when deciding whether or not to pursue a child sexual abuse report on the basis of sufficient evidence which further perpetuated a cycle of abuse and cover up. Similarly, it was highlighted that the Church in the Republic of Ireland possesses a highly influential cultural and hierarchical status due to its political significance that propagated cover up and secrecy. Despite efforts to uncover the truth, many reports failed to achieve this aim due to lack of co-operation and disclosure. Australia's response represents the most robust commitment to legal developments to effect change and hold perpetrators accountable. Criminalising omissions as

well as positive acts in the form of legal duties for professionals provides more adequate protection for children who are often in a weaker position of power.

The introduction of legal reforms and more robust action to hold perpetrators accountable is therefore necessary to create a culture of transparency and full disclosure within the Church. It has been suggested that mandatory reporting legislation would be the most effective method to do this as it will allow the government to monitor reports and trends in order to develop the most effective protection strategies to effect institutional change. Although not a 'cure' for sexual abuse, it will create a fundamental shift in the way we understand child sexual abuse and how children are treated and protected in institutions. However, implementation of mandatory reporting laws in England and Wales must be considered carefully due to the danger that a lack of an all-encompassing definition can have on enforcing mandatory reporting practices. This is particularly important in light of the recent UKSC decision which favoured a narrow interpretation as to the circumstances in which members of an organisation can be held accountable for failing to protect vulnerable victims.

Ultimately, the act of child sexual abuse should be recognised as a heinous criminal act which will only occur if legal reforms and initiatives lead to more prosecutions and convictions in order to reflect the crime's severity. It is therefore necessary to mandate reporting and create a culture of vigilance through transparent and protective policies that place the welfare of children as the paramount consideration of the Church.

---

* Maria is an LLB graduate and Trainee Solicitor currently studying at the Institute of Professional Legal Studies, Queen's University, Belfast.

[1] Independent Inquiry into Child Sexual Abuse, 'The Report of the Independent Inquiry into Child Sexual Abuse' (October 2022) <https://webarchive.nationalarchives.gov.uk/ukgwa/20221215051709/https://www.iicsa.org.uk/key-documents/31216/view/report-independent-inquiry-into-child-sexual-abuse-october-2022_0.pdf> accessed 24 June 2023.

[2] CPS, 'Child Sexual Abuse: Guidelines on Prosecuting Cases of Child Sexual Abuse' (16 June 2020).

[3] ibid.

[4] ibid.
[5] ibid.
[6] NSPCC, 'Children and the law' (17 May 2023) <https://learning.nspcc.org.uk/child-protection-system/children-the-law#article-top> accessed 24 June 2023.
[7] Social Services and Well-being (Wales) Act 2014, s3(3).
[8] NSPCC, 'Children and the law' (17 May 2023) <https://learning.nspcc.org.uk/child-protection-system/children-the-law#article-top> accessed 24 June 2023.
[9] Independent Inquiry Child Sexual Abuse, 'The Anglican Church, Case Studies: 1. The Diocese of Chichester 2. The response to allegations against Peter Ball' (May 2019) 123 <https://webarchive.nationalarchives.gov.uk/ukgwa/20221214232838/https://www.iicsa.org.uk/key-documents/11301/view/anglican-church-case-studies-chichester-peter-ball-investigation-report-may-2019.pdf> accessed 24 June 2023.
[10] ibid 111.
[11] Di McNeigh and Sara Scot, 'Key messages from research on child sexual abuse in institutional contexts' (2023) Centre of expertise on child sexual abuse 4.
[12] ibid.
[13] Faisal Rashid and Ian Barron, 'Why the Focus of Clerical Child Sexual Abuse has Largely Remained on the Catholic Church amongst Other Non-Catholic Christian Denominations and Religions' (2019) 28(5) Journal of Child Sexual Abuse 564, 575.
[14] Faisal Rashid and Ian Barron, 'Why the Focus of Clerical Child Sexual Abuse has Largely Remained on the Catholic Church amongst Other Non-Catholic Christian Denominations and Religions' (2019) 28(5) Journal of Child Sexual Abuse 564, 575.
[15] Child Rights International Network, 'Child sexual abuse in the Catholic Church' <https://home.crin.org/issues/sexual-violence/child-sexual-abuse-catholic-church> accessed 28 Jun 2023.
[16] Child Rights International Network, 'Child Abuse and the Holy See: The need for justice, accountability and reform' (2014) 5.
[17] ibid.
[18] Independent Inquiry into Child Sexual Abuse, 'The Report of the Independent Inquiry into Child Sexual Abuse' (October 2022) <https://webarchive.nationalarchives.gov.uk/ukgwa/20221215051709/https://www.iicsa.org.uk/key-documents/31216/view/report-independent-inquiry-into-child-sexual-abuse-october-2022_0.pdf> accessed 24 June 2023.
[19] NSPCC, 'Safeguarding Children and Child Protection' <https://learning.nspcc.org.uk/safeguarding-child-protection> accessed 16 November 2021.
[20] ibid.
[21] ibid.
[22] NSPCC, 'Child Protection System in the UK' <https://learning.nspcc.org.uk/child-protection-system> accessed 16 November 2021.
[23] Ian Elliott, 'A Single Safeguarding Strategy – Learning from Past Mistakes' (2014) 65 *The Furrow* 3.
[24] Temitope Ige and Esther Opeyemi Ilesanmi, 'Child Sexual Abuse in the Church: Biblo-Legal Perspective' (2021) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3830608> accessed 16 November 2021.
[25] Department of Health and Social Security, *Working Together for the Protection of Children Guidance* (1986).
[26] Children Act 2004.
[27] The Education (Independent School Standards) Regulations 2014.
[28] Children Act 1989, s1(1).
[29] Jonathan Herring, *Family Law and Relationships* (9th edn, Longman Pearson 2019) 470.
[30] *J v C* [1970] AC 668.
[31] *Re W (A Child) (Adoption: Delay)* [2017] EWHC 829 (Fam).
[32] Independent Inquiry into Child Sexual Abuse, 'Ampleforth and Downside (English Benedictine Congregation Case Study)' (August 2018) 11 <https://www.iicsa.org.uk/key-documents/6583/view/ampleforth-downside-investigation-report-august-2018.pdf> accessed 17 October 2021.
[33] Children Act 1989, s17.
[34] Independent Inquiry into Child Sexual Abuse, 'Ampleforth and Downside (English Benedictine Congregation Case Study)' (August 2018) <https://www.iicsa.org.uk/key-documents/6583/view/ampleforth-downside-investigation-report-august-2018.pdf> accessed 17 October 2021.

[35] Michael Nolan, 'A Programme for Action: Final Report of the Independent Review on Child Protection in the Catholic Church in England and Wales (the Nolan Report)' Catholic Communications Service / Catholic Bishops (September 2001) 14.
[36] ibid 1.
[37] ibid 14.
[38] 'diocese, n' (*OED Online* OUP December 2021) <https://www.oed.com/view/Entry/53084?redirectedFrom=diocese#eid > accessed 16 November 2021.
[39] 'religious order' (*Oxford Reference*) <https://www.oxfordreference.com/view/10.1093/oi/authority.20110803100413127> accessed 16 November 2021.
[40] Michael Nolan, 'A Programme for Action: Final Report of the Independent Review on Child Protection in the Catholic Church in England and Wales (the Nolan Report)' Catholic Communications Service / Catholic Bishops (September 2001) 35.
[41] Independent Inquiry into Child Sexual Abuse, 'The Roman Catholic Church Investigation Report' (November 2020) 35 <https://www.iicsa.org.uk/key-documents/23357/view/catholic-church-investigation-report-4-december-2020.pdf> accessed 17 October 2021.
[42] ibid 38.
[43] Independent Inquiry into Child Sexual Abuse, 'Ampleforth and Downside (English Benedictine Congregation Case Study)' (August 2018) 19 <https://www.iicsa.org.uk/key-documents/6583/view/ampleforth-downside-investigation-report-august-2018.pdf> accessed 17 October 2021.
[44] ibid.
[45] P Gilligan, 'Rhetoric, review and recognition: Exploring the failure of the Catholic Church in England and Wales to satisfy survivors of sexual abuse by its clergy' (2014) Workshop on Sexual Abuse in the Church and other Institutional Settings.
[46] 'Fifty-two Catholic priests defrocked in England and Wales since 2001' *The Guardian* (24 July 2014) <https://www.theguardian.com/world/2014/jul/24/catholicism-religion> accessed 17 October 2021.
[47] 'Catholic Church defrocks 52 priests for sex abuse' *BBC News* (24 July 2014) <https://www.bbc.co.uk/news/uk-28466874> accessed 17 October 2021.
[48] Faisal Rashid, Ian Barron and Jungsun Hyun, 'First Catholic Church of England and Wales safeguarding structure to protect children from Clerical Sexual Abuse: A Commentary on Nolan (2001) till Cumberlege (2007)' (2020) CIE Materials and Commentaries 10.
[49] Independent Inquiry into Child Sexual Abuse, 'Ampleforth and Downside (English Benedictine Congregation Case Study)' (August 2018) 21 <https://www.iicsa.org.uk/key-documents/6583/view/ampleforth-downside-investigation-report-august-2018.pdf> accessed 17 October 2021.
[50] ibid.
[51] Inquiry into the handling of child abuse by religious and other organizations (2012) SNAP Australia 7.
[52] Code of Canon Law, The Vatican <https://www.vatican.va/archive/cod-iuris-canonici/cic_index_en.html> accessed 17 October 2021.
[53] 'canon law' (*Collins English Dictionary*) <https://www.collinsdictionary.com/dictionary/english/canon-law> accessed 17 October 2021.
[54] ibid.
[55] Inquiry into the handling of child abuse by religious and other organizations (2012) SNAP Australia 7.
[56] Timothy Willem Jones, 'Sin, Silence and States of Denial: Canon Law and the 'Discovery' of Child Sexual Abuse' 41(2) Australian Feminist Law Journal 237, 243.
[57] Code of Canon law, CIC83, can 1752.
[58] Timothy Willem Jones, 'Sin, Silence and States of Denial: Canon Law and the 'Discovery' of Child Sexual Abuse' 41(2) Australian Feminist Law Journal 237, 243.
[59] Sexual Offences Act 2003, s9.
[60] Independent Inquiry into Child Sexual Abuse, 'Ampleforth and Downside (English Benedictine Congregation Case Study)' (August 2018) <https://www.iicsa.org.uk/key-documents/6583/view/ampleforth-downside-investigation-report-august-2018.pdf> accessed 17 October 2021.
[61] ibid.
[62] ibid 43.
[63] Inquiry into the handling of child abuse by religious and other organizations (2012) SNAP Australia 7.
[64] Michael D White and Karen J Terry, 'Child sexual abuse in the Catholic Church: Revisiting the rotten apples explanation' (2008) 35(5) *Criminal Justice and Behavior* 663.
[65] Donald Cozzans, 'Clerical celibacy: The heritage' (2006) 60(3) *Interpretation* 356-357.

[66] Geoffrey Robinson, *Confronting Power and Sex in the Catholic Church: Reclaiming the Spirit of Jesus* (Liturgical Press 2008).
[67] Faisal Rashid, Ian Barron and Jungsun Hyun, 'First Catholic Church of England and Wales safeguarding structure to protect children from Clerical Sexual Abuse: A Commentary on Nolan (2001) till Cumberlege (2007)' (2020) CIE Materials and Commentaries 13.
[68] M. R. Gula 'A professional code of ethics? Church Ethics and Its Organizational Context: Learning from the Sex Abuse Scandal in the Catholic Church' (2006) 12 *Boston College Church in the 21st Century Series* 147-156.
[69] Daniel Coquillette and Judith McMorrow, 'Towards an ecclesiastical professional ethic: Lessons from the legal profession' (2005) 65 Boston College Law School Legal Studies Research Paper Series 9.
[70] Faisal Rashid, Ian Barron and Jungsun Hyun, 'First Catholic Church of England and Wales safeguarding structure to protect children from Clerical Sexual Abuse: A Commentary on Nolan (2001) till Cumberlege (2007)' (2020) CIE Materials and Commentaries 13.
[71] Sexual Offences Act 2003, ss5-15A.
[72] Sexual Offences Act 2003, s22(3)(a).
[73] Sexual Offences Act 2003, s22(3)(b).
[74] HC Deb 3 March 2021, vol 690, col 357.
[75] thirtyone:eight is an independent Christian charity that specialises in safeguarding to protect vulnerable people from abuse.
[76] thirtyone:eight, *Positions of Trust: it's time to change the law* (2020) 23.
[77] Crimes Act 1958, 37(1)(i).
[78] HC Deb 3 March 2021, vol 690, col 360.
[79] ibid.
[80] European Convention on Human Rights, Article 8.
[81] thirtyone:eight, *Positions of Trust: it's time to change the law* (2020) 23.
[82] 'Police, Crime, Sentencing and Courts Bill 2021: positions of trust factsheet' (7 July 2021) <https://www.gov.uk/government/publications/police-crime-sentencing-and-courts-bill-2021-factsheets/police-crime-sentencing-and-courts-bill-2021-positions-of-trust-factsheet> accessed 2 January 2022.
[83] thirtyone:eight, *Positions of Trust: it's time to change the law* (2020) 26.
[84] ibid.
[85] Karen Terry, 'Child sexual abuse within the Catholic Church: a review of global perspectives' (2015) 39 2 International Journal of Comparative and Applied Criminal Justice 139, 140.
[86] Mary Gail Frawley-O'Dea, 'The History and Consequences of the Sexual-Abuse Crisis in the Catholic Church' (2004) 5 1 Studies in Gender and Sexuality 11, 12.
[87] Bishops Ad Hoc Committee on Sexual Abuse, *Restoring Trust: A Pastoral Response to Sexual Abuse* (National Conference of Catholic Bishops 1994).
[88] ibid.
[89] Charter for the Protection of Children and Young People Revised Edition 2002, Preamble.
[90] Mary Gail Frawley-O'Dea, 'The History and Consequences of the Sexual-Abuse Crisis in the Catholic Church' (2004) 5 1 Studies in Gender and Sexuality 11, 15.
[91] Karen Terry, 'Child sexual abuse within the Catholic Church: a review of global perspectives' (2015) 39 2 International Journal of Comparative and Applied Criminal Justice 139, 143.
[92] ibid 140.
[93] The Office for National Statistics, *Child Sexual Abuse in England and Wales: Year Ending March 2019* (2020) 6. <https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/childsexualabuseinenglandandwales/yearendingmarch2019> accessed 2 January 2022.
[94] ibid.
[95] David Clohessy, 'Tired of the drip, drip, drip of Catholic sexual abuse reports? Let's try this' (National Catholic Reporter, 11 August 2021) <https://www.ncronline.org/news/accountability/tired-drip-drip-drip-catholic-sexual-abuse-reports-lets-try> accessed 17 December 2021.
[96] ibid.
[97] ibid.
[98] ibid.
[99] Independent Inquiry into Child Sexual Abuse, 'Accountability and Reparations' Investigation Report (September 2019)

<https://webarchive.nationalarchives.gov.uk/ukgwa/20221215042324/https://www.iicsa.org.uk/key-documents/14231/view/accountability-reparations-report-19-sep-2019.pdf> accessed 24 June 2023.
[100] Limitation Act 1980, s33.
[101] Limitation Act 1980, s33(3)(a).
[102] Linda Hogan, 'Clerical and Religious Child Abuse: Ireland and Beyond' (2011) 72 Theological Studies.
[103] Anne-Marie McAlinden, 'An inconvenient truth: barriers to truth recovery in the aftermath of institutional child abuse in Ireland' (2013) 33 2 Legal Studies 189, 193.
[104] Eoin Daly, 'Re-Evaluating the Purpose of Church-State Separation in the Irish Constitution: The Endowment Clause as a Protection of Religious Freedom and Equality' (2008) 2 Judicial Studies Institute Journal 86, 91.
[105] *Norris v Attorney General* [1984] IR 36 [64].
[106] 'Sexual abuse, exploitation of women and paedophile priests: the scandals that have rocked the Catholic Church' *Independent* (26 August 2018) <https://www.independent.ie/irish-news/pope-francis-in-ireland/sexual-abuse-exploitation-of-women-and-paedophile-priests-the-scandals-that-have-rocked-the-catholic-church-37245419.html> accessed 19 December 2021.
[107] 'Cardinal Brady 'failed to act on sex abuse claims'' *BBC News* (2 May 2012) <https://www.bbc.com/news/uk-northern-ireland-17894419> accessed 19 December 2021.
[108] 'Sexual abuse, exploitation of women and paedophile priests: the scandals that have rocked the Catholic Church' *Independent* (26 August 2018) <https://www.independent.ie/irish-news/pope-francis-in-ireland/sexual-abuse-exploitation-of-women-and-paedophile-priests-the-scandals-that-have-rocked-the-catholic-church-37245419.html> accessed 19 December 2021.
[109] Augustine Pang, Eada Hogan, Igor Andrasevic, 'The Catholic Church abuse scandal in Ireland: two steps forward, one step back by Pope Francis?' (2021) Corporate Communications: An International Journal.
[110] Anne-Marie McAlinden, 'An inconvenient truth: barriers to truth recovery in the aftermath of institutional child abuse in Ireland' (2013) 33 2 Legal Studies 189, 194.
[111] Fionnan Sheahan, 'Albert's resignation as Taoiseach could not be stopped, says Bertie' *Independent* (22 August 2014) <https://www.independent.ie/irish-news/news/alberts-resignation-as-taoiseach-could-not-be-stopped-says-bertie-30530161.html> accessed 19 December 2021.
[112] *Everson v Board of Education* (1947) 330 US 1.
[113] Linda Hogan, 'Clerical and Religious Child Abuse: Ireland and Beyond' (2011) 72 Theological Studies 170, 175.
[114] In 2000, the Commission to Inquire into Child Sexual Abuse was established by the Irish government to investigate abuse of children in institutions.
[115] Anne-Marie McAlinden, 'An inconvenient truth: barriers to truth recovery in the aftermath of institutional child abuse in Ireland' (2013) 33 2 Legal Studies 189, 196.
[116] Criminal Justice (Withholding of Information on Offences Against Children and Vulnerable Persons) Act 2012.
[117] Criminal Justice (Withholding of Information on Offences Against Children and Vulnerable Persons) Act 2012, ss2(1)(a) and 2(1)(b).
[118] Children First Act 2015, s14.
[119] Ashling Bourke and Catherine Maunsel, 'Teachers Matter': The Impact of Mandatory Reporting on Teacher Education in Ireland' [2015] 25 Child Abuse Review 314, 315.
[120] ibid.
[121] Department of Children and Youth Affairs, *Children First National Guidance for the Protection of Welfare and Children* (2017) 26.
[122] ibid.
[123] Anne-Marie McAlinden, 'An inconvenient truth: barriers to truth recovery in the aftermath of institutional child abuse in Ireland' (2013) 33 2 Legal Studies 189, 197.
[124] The Bichard Inquiry Report (2004, HC 653).
[125] Health Service Executive, *Safeguarding Vulnerable Persons at Risk of Abuse National Policy and Procedures* (2014).
[126] Katie Wright, Shurlee Swain and Kathleen McPhillips, 'The Australian Royal Commission into Institutional Responses to Child Sexual Abuse' (2017) 74 Child Abuse & Neglect 1.
[127] Crimes Act 1958, s327.
[128] ibid, s327(2).
[129] Crimes Act 1900, s316(a).
[130] ibid, s316(b).

[131] 'Archbishop Philip Wilson sentenced for concealing child sex abuse' *BBC News* (3 July 2018) <https://www.bbc.co.uk/news/world-australia-44692396> accessed 14 January 2022.
[132] *R v Wilson* [2018] NSWDC 487 [85].
[133] Tony Foley, 'Changing institutional culture in the wake of clerical abuse – the essentials of restorative and legal regulation' 22(2) (2019) Contemporary Justice Review 171, 179.
[134] *R v Wilson* [2018] NSWDC 487 [94].
[135] Crimes Act 1900, s316A.
[136] Tony Foley, 'Changing institutional culture in the wake of clerical abuse – the essentials of restorative and legal regulation' 22(2) (2019) Contemporary Justice Review 171, 179.
[137] Ben Matthews, Strengthening Mandatory Reporting of Child Sexual Abuse in Europe: A Study Setting the Scene for Further Action Responding to Violence against Children, Strasbourg: Council of Europe, 2020. CDENF-GT-VAE(2020)02.
[138] Ben Matthews, Xing Ju Lee and Rosana E Norman, 'Impact of a new mandatory reporting law on reporting and identification of child sexual abuse: A seven-year time trend analysis' 56 (2016) *Child Abuse and Neglect* 62-79.
[139] Social Services and Well-Being (Wales) Act 2014, s130.
[140] Ben Matthews, 'A model law for the mandatory reporting of child sexual abuse in England and Wales: Submission to the independent inquiry into child sexual abuse' (2020) Brisbane, Queensland University of Technology.
[141] ibid.
[142] *Trustees of the Barry Congregation of Jehovah's Witnesses v BXB* [2023] UKSC 15 [68].
[143] ibid [74].
[144] ibid [76].
[145] Children and Young Persons (Care and Protection) Act 1998, ss23 and 27
[146] Children, Youth and Families Act 2005, s182(1)(ea).
[147] Children and Young People Act 2008, s356.
[148] Ben Matthews, 'A taxonomy of duties to report child sexual abuse: Legal developments offer new ways to facilitate disclosure' (2019) 88 Child Abuse and Neglect 337, 343.
[149] Ben Matthews, 'A taxonomy of duties to report child sexual abuse: Legal developments offer new ways to facilitate disclosure' (2019) 88 Child Abuse and Neglect 337, 344.
[150] Martha Nussbaum, 'Creating Capabilities: The Human Development Approach and Its Implementation' (2009) 24(3) Hypatia 211-215.
[151] 'Pope Francis sets up Vatican child sex abuse committee' *BBC News* (5 December 2013) <https://www.bbc.co.uk/news/world-europe-25235724> accessed 20 December 2021.
[152] ibid.
[153] 'Pope Francis compares child sex abuse to human sacrifice' *BBC News* (24 February 2019) <https://www.bbc.co.uk/news/world-europe-47348479> accessed 22 December 2021.
[154] 'Vatican laws changed to toughen sexual abuse punishment' *BBC News* (1 June 2021) <https://www.bbc.co.uk/news/world-europe-57318959> accessed 22 December 2021.
[155] Independent Inquiry into Child Sexual Abuse, 'The Roman Catholic Church Investigation Report' (November 2020) <https://www.iicsa.org.uk/key-documents/23357/view/catholic-church-investigation-report-4-december-2020.pdf> accessed 9th January 2022.
[156] Catherine Pepinster, 'Five years on, Pope Francis has failed to deliver on his promises' *The Guardian* (12 March 2018) <https://www.theguardian.com/commentisfree/2018/mar/12/pope-francis-catholic-church-child> accessed 20 December 2021.
[157] Marie Collins, 'Exclusive: Survivor explains decision to leave Vatican's abuse commission' *The National Catholic Reporter* (1 March 2017) <https://www.ncronline.org/news/people/exclusive-survivor-explains-decision-leave-vaticans-abuse-commission> accessed 17 October 2021.
[158] ibid.

A COMPARISON OF HONG KONG'S PDPO AND THE EUROPEAN UNION'S GDPR IN THE CONTEXT OF THE UNITED KINGDOM'S DPA 2018

ALEXANDER J.D GARMENT[*]

Abstract

Data protection is an active, growing and ever more important area of law. Consequently, it is pertinent to analyse how different regimes operate so that we can formulate a better understanding of how these regimes protect our privacy in their individual contexts. A comparison between regimes also offers the opportunity to examine how regimes may differ in their origins, purpose and the protection offered, thereby allowing a deeper understanding of what data protection is and should be. This article will focus on the GDPR as implemented by the United Kingdom's (UK) Data Protection Act 2018 and Hong Kong's Personal (Privacy) Data Protection Ordinance (PDPO) 1996. Hong Kong being a former colony of the UK has retained many facets of the UK legal system, and therefore, offers a similar context in which the legal regime is formulated and operates. Equally, with both jurisdictions being important financial hubs, there is a similar enough context to make a comparison worthwhile, thus allowing the article to focus upon the two legal regimes and their difference in doctrine and functionality. This comparison will be conducted using a functionalist methodology, utilising a micro-comparison approach. This will enable an examination of the functionality of the regimes, thus providing greater insight than what a purely doctrinal analysis can offer. This article will demonstrate that despite being younger, and more business orientated than the human rights-approach of the GDPR, Hong Kong's PDPO functionally offers similar levels of protection in many of the core facets of data protection while being doctrinally dissimilar. However, if Hong Kong wishes to maintain its role as a financial hub in Asia, its data protection regime needs to continue to develop so that it can adequately respond to the demands modern society and technology place on it.

INTRODUCTION

Data protection regimes have been gathering pace and importance in the public psyche since the 1980s, especially with the introduction of the OECD Privacy Guidelines[1] in response to growing technological demands on data collection, storage, processing and privacy. This has culminated thus far with the introduction of the European Union General Data Protection Regulation[2] (GDPR) passed in 2016 and entered force in 2018. The 1980s was a decade of data privacy legislation with the enactments of the OECD guidelines closely followed by the European Council's Convention 108,[3] and consequently numerous national legislation. This short exploration of data protection history is important to note, as the principles formulated during this time form a foundational base upon which much of the global data protection regimes can trace a common ancestry to. The principles of collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability form the core of data protection,[4] threading a common theme that underpins subsequent legislation. This consequently means when comparing data protection legal regimes there will be undoubtedly similarities found; however, from these core principles, the actual functionality of data regimes often differ. This article will focus on the EU GDPR in the form of the United Kingdom's implementation via the Data Protection Act 2018 (DPA)[5]– which implements the UK GDPR as per the EU exit amendments– and comparatively analysing it against Hong Kong's Personal Data (Privacy) Ordinance (PDPO).[6] It should be noted that since the UK implemented the GDPR as per its legal obligation, by transposing it into national legislation post-Brexit means there may be eventual divergences as the EU continues to issue Directives which aim to provide frequent updates to the regulation. However, as will be noted throughout this article, this divergence will not be massive, with states outside of the EU in many ways having to reform data protection regimes in such a way that they converge with the EU regime. This is a

consequence of the EU GDPR data sharing requirements and the importance of the EU bloc as a global hub in trade and finance.

The comparison between Hong Kong and the DPA is a justifiable comparison on several grounds. Firstly, Hong Kong being a former colony has close ties to the UK legal system, having retained its common law system and echoing the 'normative' legal structures found in the UK. Secondly, in combination with the first point, with London being a major financial hub, and Hong Kong equally an important financial hub, there is a strong similarity in context. These similarities are important for fostering a comparative analysis as the more common ground that can be established, the more numerous and richer the issues which lend themselves to a comparative analysis there will be.[7] On another level, the similarity in context yet the presence of two different data protection regimes makes for an interesting analysis of how well they function in protecting individuals living in similar contexts. Furthermore, this comparison was chosen as Hong Kong has a relatively robust and established data protection regime, originating at the same time as the EU Directive 95/46[8] and based on the OECD guidelines from 1980 which outlines principles found commonly across OECD member states national legislation of which the UK is (the EU also being an active participant even though not a member itself as an organisation). Gerhard Dannemann states, there is no point comparing what is identical and what has nothing in common.[9] Equally, Dannemann argues that there must be a minimum number of differences to make a comparison worthwhile.[10] Hong Kong and the UK offer a golden option with similar contexts yet differing approaches to data protection.

This article will explore and analyse the two data protection regimes by primarily focusing on data protection in the context of media/social media and digital marketing. However, first, there will be a discussion of methodology and how the comparison between legal frameworks is to occur, followed by an initial broader comparison of the two regimes.

1. COMPARATIVE LAW

1.1 The Functionalist Methodology

Within the field of comparative law, there are numerous approaches which one can take– for instance, functionalism, structuralism and contextualism. This article will utilise what Ralf Michaels termed the mantra of comparative law–the functional method. The functional method entails a focus on the effect of the rules and events that regimes have. Functionalists analyse how legal systems compare by considering their various judicial responses to similar situations,[11] shifting away from a macro-comparison– an analysis of general questions and generally doctrinal focused–, to a micro-comparison which focuses on specific legal problems.[12] Furthermore, functionalism aims to cast light 'on the relationship between law and society'.[13] This is an equally important aspect of this articles purpose. Law does not exist in isolation to societal, economic and political developments. Law is in itself a functional and changing facet of modern society. To analyse and attempt to compare legal regimes properly, it is necessary to factor in the relationship between law and society. Moreover, the focus is placed on the effects of rules rather than doctrinal structures and arguments.[14] This is the primary objective and approach undertaken by this article; how functionally equivalent is the PDPO to the GDPR and what implication is there if it fails to be functionally equivalent? However, as is undertaken in section 2, a brief, more doctrinal focused comparison occurs as it would be remiss to not undertake such a comparison to ascertain some basic familiarity with the two regimes to be critically compared. This article therefore will explore, following a brief overview, a comparison between the PDPO and the DPA through case law that highlight how the frameworks operate in practice. As Pierre Legrand notes, the law is not just the words found in legal texts.[15] There is a

need to consider the function of the application of the rule by its interpreter making it necessary to explore context-specific applications of legal regimes.[16]

While Legrand is not a functionalist, his arguments are cognisant for this articles functionalist approach. Contextual comparative law is not necessarily a reaction against functionalism.[17] The contextual methodology aims to correct the 'exaggerations of the functional method, leaving room for engagement with real-world issues and providing feasible pragmatic solutions while remaining aware of the facts behind the law'.[18] Uwe Kischel's argument does not suggest that functionalism and contextualism cannot coexist. Kischel instead suggests that the contextual approach can be supplementary or corrective to functionalism.[19] The functional methodology is not a clear method, with there existing a range of methods which fall under its umbrella.[20] While this article primarily adheres to the 'classical' functionalist method, it is acknowledged the importance of context in generating insightful and meaningful comparison. Further to this, law is not isolated from politics, economics and societal developments, meaning per Michaels, law adapts to social needs.[21] As Michaels outlines, comparative law in the form of adaptionism, acts as a science of how societies deal with similar problems on their path towards progress.[22] This article therefore recognises the need for contextualism and attempts to utilise a primarily functionalist methodology strengthened by elements of contextualism.

Another important aspect of comparative law is the search for harmonisation of legal regimes.[23] Part of this search for harmonisation manifests itself in transplants or convergence. Legal transplants occur when legislators enact new laws that largely follow the structures of law from another country.[24] Convergence is the gradual process whereby there is a growing similarity between two systems. Matthias Siems crucially states that this does not mean that they will become or are identical, but rather are trending towards greater similarity.[25] This article will discuss the process of convergence, more so than transplants, and the role GDPR has played in

potentially directing data protection regimes towards a common form. Within this process of convergence, it will be important to keep in mind the force of globalisation. Horatia Watt poses the question of whether globalisation is the death of comparative law[26]– if all data protection becomes the same in form then the activity of comparison becomes pointless as Dannemann highlighted earlier. However, this is mitigated by the fact that, while the laws as written may appear the same, their function within society often differ on some level, whereby we can then glean knowledge and perspective as to how data protection regimes interact within different contexts. Watt offers the alternative view to death of comparison in the face of total harmonisation, suggesting the term covers up developments which could be understood best as parallel but indigenous processes.[27] For this article, it is important to keep this in mind when analysing Hong Kong's data protection regime, especially when considering future developments.

1.2 Functionalism Critique

While the functional approach has been a dominant methodology within comparative law there have been many criticisms. Dannemann highlights that the functionalist approach typically focuses on either similarities or differences in its search for the harmonisation of law. But obviously, there is a need to strike a balance between differences and similarities, with the balance struck depending on the purpose of the comparative enquiry.[28] Dannemann critiques this focus on similarities by providing the warning that a search for similarities can lead to finding superficial similarities providing the example that all judges should be independent.[29] However, by using a micro-comparison approach and delving into cases highlighting different aspects of how data protection regimes operate in the two contexts, it will be possible to bring to the fore differences and similarities that only appear following deeper analysis. It is important not to fall

into what Watt termed the 'twin illusions of similarity (differences are negligible) and ease (any difference there are may easily be overcome), which are recurrent temptations with comparative scholarship itself.'[30] Equally, there is a need to analyse the differences and similarities without giving a verdict as to 'which-is-best', as a pursuit of this nature can lend itself to reductionism and oversight of key aspects of each legal regime. For instance, the underlying contexts behind each regime has a significant impact on how the regime functions in practice.

The GDPR, and consequently the DPA, is at heart a document protecting a human right to privacy. Hong Kong's PDPO was enacted in 1996 and based on the OECD privacy guidelines (1980) with the intention of providing adequate data protection to retain its status as an international trading centre and give effect to human rights treaty obligations. The PDPO is therefore more business-orientated than the GDPR. This is not surprising. The UK Data Protection Act 1984, which originates from the same period as other frameworks relied upon by the PDPO, as Andrew Charlesworth notes, also does not consider human rights as being an important aspect.[31] These differences in purpose will become apparent when examining each data protection regime through a micro-comparison.

Structuralism and contextualism offer alternatives as methodologies through which to engage with the exercise of comparing legal regimes. As highlighted by Geoffrey Samuel, the functionalist approach does not offer an explanation of the internal structures of a legal system and how these structures came into being.[32] Structuralism offers a solution as it allows the observer to focus on the structures hidden within the phenomenon being observed.[33] Fundamentally, structuralism focuses on the underlying system.[34] For instance, it discusses the European system of law– described as an 'institutional system'– and the UK 'normative system', as points from which to draw comparisons with other jurisdictions and systems.[35] While this approach offers new and valuable insights for comparatists without the risk of 'imposing on the

"other" legal system',[36] it is more appropriate for a macro-comparison. Individual details would become lost within this 'system' based comparison. Furthermore, as Hong Kong inherited its current legal system from the UK – as noted in the introduction–, it would be, for the purposes of this article, unproductive when attempting to understand the particular functionality of two legal regimes – the PDPO and GDPR/ DPA– but within two relatively similar legal systems.

2. AN INITIAL COMPARISON

This section will explore a brief overview of the two regimes through a discussion of the scope of the regulations, the role of the privacy Commissioner, and accountability and sanctions. It offers an opportunity to explore and compare the black-letter law of the two regimes, thereby forming an initial understanding of the differences and similarities from which a deeper analysis can be formed. Critically, the following initial comparison enables the avoidance of the simplistic exercise of identifying similarities and differences during the functionalist micro-comparison in the later sections. Moreover, it provides an opportunity for the identification of potential convergence and/or harmonisation of the two regimes at a first instance alongside a critical analysis of how the regimes discuss some of the core aspects of data protection.

2.1 Scope of Regulation

Differences between the DPA and PDPO when comparing purely black-letter law, can mainly be explained by a degree of refinement. The EU has in some form been developing data privacy laws since 1981. This culminated in Directive 95/46[37] and eventually the GDPR, alongside several different Directives focused on various issues faced by data privacy. This process and the number of cases filed concerning each framework – for example, *Google Spain v AEPD* [38] and the

reclassification of internet service providers as data processors, thus furthering the functionality of Directive 95/46–, means the data protection regime has been steadily refined. The DPA and UK GDPR are, unsurprisingly, therefore, one of, if not the most, comprehensive and extensive data privacy protection frameworks globally. Hong Kong, on the other hand, is a much younger framework, having been first formulated in 1995 and enacted in 1996, being primarily based on the OECD guidelines on privacy– an important publication in data privacy law despite being non-binding– and the EU Directive 95/46. However, while it may be younger and lack the extensive case law allowing refinement to the same level as the EU regime, Hong Kong's data protection laws have developed rapidly and in keeping with the new threats posed by technological developments. For instance, in 2021 the PDPO was amended to make doxing a specific crime. Doxing is the phenomenon whereby 'individuals or groups search for and publish private or identifying information [...] on the internet, typically with malicious intent'.[39] This is perhaps principally due to Hong Kong's PDPO being based on a need to retain its position as a leading financial hub in the face of a wave of doxing incidents.[40] This naturally means providing extensive laws and regulations which promote trust and thus investment and financial activity. Furthermore, it this form of regulatory evolution that is required if jurisdictions outside of the EU wish to continue to be able transfer data with the EU.

2.2 The Commissioner

The DPA and Hong Kong's PDPO have a couple of similarities. Firstly, they both highlight similar core data protection principles (DPPs) which underpin the data protection regime– The lawful and fair collection of data; purposeful and necessary; accuracy; consent; security of data; access to data.[41] The regimes also both require the establishment of an independent supervisory authority that oversees the implementation of the data protection regime.[42] Under both regimes,

the Commissioners hold similar functions such as monitoring compliance, promoting and writing codes of practice and undertaking inspections.[43] One difference in operation is the powers the Commissioner holds when undertaking an investigation. Under s. 42 of the PDPO the Commissioner can inspect a premises once 14 days' notice has been given. The privacy Commissioner can also issue cessation notices under the 2012 amendments. The UK commissioner, on the other hand, must gain a warrant through the courts before being able to undertake a premises search.[44] The PDPO thus grants greater power and leverage directly to the Commissioner, making it theoretically easier for the Commissioner to conduct investigations and thus protect individual's data. However, this greater power is more difficult to trigger, as unlike the DPA[45] there is no requirement for a data user to inform the office of the Privacy Commissioner of a breach, instead relying on it being reported by an individual affected by the breach.[46] This is a significant weakness of the PDPO. However, the Hong Kong Privacy Commissioner in a 2023 briefing reported that concrete proposals were being developed to implement a mandatory data breach notification mechanism.[47] If the PDPO is amended to include this obligation this would be a significant step towards improving data protection within Hong Kong. It would equally, indicate convergence with the GDPR, thus further cementing how significant and formative the GDPR is for data protection regimes with it acting as a regime against which to test adequacy. The test of adequacy under the EU GDPR as a requirement for data sharing, which has an important role within global business and security dealings, is a strong influencing factor for eventual convergence. It should be noted that, while it may not be a mandatory requirement in Hong Kong, many companies often do file notifications of data breaches.[48] This most likely occurs as companies attempt to foster good public relations, thus increasing trust and better business. The PDPO to be amended to include mandatory reporting would be a necessary strengthening of Hong Kong's data ordinance if it wishes to continue serving as a major financial hub. The voluntary reporting that currently operates which relies on

companies self-reporting instances of data breaches is a significant weakness which undermines the PDPO and authority given to the commissioner.

2.3 Accountability And Sanctions

Generally speaking, the PDPO offers far less accountability than the DPA. Alongside no current mandatory notification mechanism, there is no obligation to conduct a data protection impact assessment or have a designated data protection officer when applicable. Furthermore, perhaps the biggest difference in generating compliance and accountability is the difference in penalties that can be awarded. The DPA under s. 157(5) and (6), states the maximum fine if a breach of the basic principles of data collection and processing of data subject rights occurs is GDP 17.5 million or 4% of annual global turnover; or, if the data processor or controller breaches their obligations there is a fine of GDP 8.7 million or 2% of global annual turnover. The PDPO has much lower fines in the case of breaches of duties and obligations. The maximum fine possible is HKD 1 million (equating to roughly GDP 100,00) and a prison sentence of up to 5 years for disclosing personal data obtained without consent to gain money or cause loss of money of the data subject.[49] Disclosure of data without consent with intent to cause harm or being reckless carries a fine of HKD 100,000 and up to 2 years imprisonment.[50] Lastly, if a breach of direct marketing rules occurs but not for personal gain then a fine of HKD 500,00 and up to 3 year imprisonment can be imposed.[51] It is important to note, while the maximum fine under the DPA is applicable for a breach of data principles, under the PDPO there is no possibility for a breach of the DPPs themselves, with a contravention of the provisions of the PDPO which are closely related and based upon the DPPs required.[52] Due to the distinctly smaller financial fines imposed by the PDPO, some commentators have suggested that the PDPO has ‘smaller teeth’ than the GDPR.[53] This could be emblematic of Hong Kong being a ‘privacy pragmatist’, with its legal regimes and

reforms driven largely by business considerations and not wishing to impose too onerous fines that could cause businesses to relocate.[54] However, unlike the UK GDPR, the PDPO introduces the possibility for prison sentences, meaning while the financial consequences are much lower, there is still a strong deterrent for breaching the regulations,

Through the above initial comparison, it is clear that while the two regimes share at the core some common basics such as the data protection principles, due to the difference in approach – fundamental rights, human rights approach versus a more business-orientated legal landscape– the actual implementation of these core DPPs are not. As will be discussed further, the two regimes implementation demonstrates a wide gap in coverage over data protection. It should be noted that the Office for the Commissioner of Privacy in Hong Kong issued guidance following the ratification of the GDPR, stating that given Hong Kong's legislation was based on OECD guidelines and Directive 95/46, with the GDPR constituting a significant development of data protection, the new framework includes several requirements not found under the PDPO.[55] It is therefore a natural consequence that the PDPO in many ways will diverge with the GDPR, and in some instances offer less protection for individuals. The 2021 doxing amendment and announced plans such as mandatory reporting are therefore important developments for the PDPO and would bring it more in line with the GDPR thereby helping Hong Kong maintain its role as a financial hub. Nonetheless, it will crucially remain different due to the underlying different approach – business-orientated/compliance vs human rights– but still achieve similar or comparable protection.

3. DEFINITION OF KEY CONCEPTS AND EFFECT ON THE FUNCTIONALITY OF DATA PROTECTION REGIME

Having established points of initial comparison, this article will now explore a deeper analysis of the PDPO and the GDPR. Key to the functionality and effectiveness of any regime are the definitions given to terms as without practical definitions the regimes can become obsolete. Especially within the fast-moving space of technology and data protection, definitions that are not flexible enough will become impractical and thus lead to the failure of the data protection regime. For instance, as discussed by W. Kuan, Julia Hörnle and Christopher Millard, cloud computing posed difficult questions for the EU Directive 95/46 and how it defined data controller and processing.[56] Consequently, the GDPR which replaced Directive 95/46 cited cloud computing as a significant reason for the need for reform to ensure that the effectiveness of data protection would not be undermined.[57] The followings section will explore how the two regimes define consent and personal data and how these definitions operate to generate a (dis)functional data protection regime.

3.1 Defining Consent

A key driver and aspect of the DPA is consent, with the standard having been significantly increased. The UK GDPR defines consent as needing to be freely given, specific, informed and evidenced by clear affirmative verifiable action before any data could be collected and processed lawfully.[58] Michelle Goddard remarks that the GDPR generally is user-centric and thus moves consent away from being purely a legal tick-boxing process.[59] On the other hand, consent under the PDPO is not so strictly defined. There is no specific definition within the PDPO providing a clear definition of what consent means. Rather, within provisions of the PDPO certain sections, for instance those on direct marketing, contain extra conditions for the need to obtain consent before undertaking that activity.[60] However, an analysis of case law provides a clearer picture of how consent is conceived under the PDPO. In the case of *Cathay Pacific Airways Ltd v*

Administrative Appeals Board & Privacy Commissioner for Personal Data,[61] in which employees reported Cathay Pacific's requirement to be given access to an employee's health record to the Commissioner, the court noted that the PDPO never required that the consent given by data subject be based on complete freedom of choice 'unburdened by any possible adverse consequences'.[62] The Court further elaborated that data protection principle 1(3) only required the data subject be fully informed on or before the start of data collection and the consequences for not complying.[63] Further to this in the case *Eastweek Publisher Ltd v Privacy Commissioner for Personal Data,*[64] the Court overturned the Commissioner's investigation conclusion that data had been unfairly collected and led to an intrusion of privacy.[65] The case centred on the photographing of six women who had not consented and the publishing of these images in a magazine. The Court ruled that as the publisher had never intended to reveal the identity of the women, the data was not personal data and thus there was no requirement for consent to be obtained for the photos to be published.[66]

It is clear therefore that the PDPO has a very different functioning conception of consent to that of the UK GDPR whereby far less protection is offered to a data subject over the collection of personal data. The Privacy Commissioner of Hong Kong noted this in a report in 2008 in which they stated that currently, Hong Kong operates an opt-out mechanism, with the need to explore and eventually implement the far stronger and better privacy-affording opt-in system that the GDPR offers.[67] This report was issued following the revelation that Octopus Rewards– a major company within Hong Kong as it operates aspects of ticketing for the MTR (the public transport company in Hong Kong)– had sold 2 million people's data for monetary gain without their knowledge or consent.[68] In 2012, an amendment to the PDPO meant that direct marketing, such as the Octopus Reward scandal, was explicitly regulated. The amendment meant that data could only be sold if consent had been given and the data subject informed if there is to be a transfer of data,[69] thus strengthening an individual's control over data. Naula O'Connor and Alethea Lange

note that there is no such thing as free usage on the internet, rather the payment instead of cash is user data.[70] In this information age, there is a growing digital marketplace where the most valuable commodity is personal data.[71] This is one reason why there is such a need for data protection and the creation of digital privacy whereby one has the 'ability to shape one's own online identity and decide when, how, and when to share parts of that identity with people' and companies.[72]

This was again brought to the forefront of data protection by the rise of doxing. In response to this growing concern, Hong Kong implemented in 2021 specific doxing amendments to the PDPO, making it an offence to disclose data which was obtained without consent and disclosed to cause distress or monetary gain.[73] In doing so, Hong Kong became one of a few jurisdictions which has enacted doxing specific legislation – joining some US states, South Korea and China–, putting the PDPO at the forefront of global data protection development. Incidentally it can be noted that the UK does not have specific anti-doxing legislation. The PDPO provision highlights the importance of the need for consent when undertaking data collection, processing and dissemination. The amendment furthers Hong Kong's data protection by creating another specific instance through which personal data is protected from misuse. As Marjia Boban states it is the modern state's obligation to ensure the protection of citizens' personality and dignity from various forms of misuse of their personal data.[74]

These developments firstly demonstrate how the PDPO is being amended to respond to technological developments by gaining stricter definitions on consent, and secondly converging with the GDPR so to afford adequate protection of people's privacy. Nonetheless, by being less flexible in definition and only advancing the legal protection afforded to individuals once a scandal or data protection concern arises, it unnecessarily places at risk all individuals and their privacy/personal data.

3.2 Defining Personal Data

Another integral aspect of any data protection regime is how it defines personal data. The DPA defines personal data as 'any information relating to an identified or identifiable living individual'.[75] This is broken down into two categories: sensitive data and ordinary data. Data that comes under sensitive data, such as racial identity or genetic material, is not to be processed unless there is an exception as listed under art. 9(2) of the UK GDPR. Due to the sensitivity of the data, there are greater risks and thus a requirement to be handled more carefully to ensure that data protection of the data subject is maintained. Further to this, the requirement to undertake a data protection impact assessment when collecting or processing data that itself poses risks or the processing is risky provides greater protection to the data subject.[76]

The PDPO defines personal data as any data '(a)relating directly or indirectly to a living individual; (b)from which it is practicable for the identity to be directly or indirectly ascertained; and (c) in a form in which access to or processing of the data is practicable'.[77] At first glance, this definition allows for a narrower conception of personal data due to the need to meet the criteria listed in (a)-(c). As was seen in the *Eastweek* case, the control over personal data is severely limited by this narrow definition. Anne Cheung highlights this when succinctly stating it is difficult to prove data collected falls within the definition of personal data when discussing the limitations of the PDPO.[78] The PDPO also differs from the DPA as there is no 'sensitive data' category within the ordinance. However, the Commissioner has referred to certain pieces of data being 'sensitive' such as the Hong Kong ID card in investigations due to the information linked to the card.[79] Nonetheless, the absence of the requirement to not process certain types of personal data does leave individuals vulnerable. As demonstrated by the aforementioned case of *Cathay Pacific*, under the GDPR the data would be designated sensitive and would therefore be difficult

to access/process without specific consent from the individual. The case would have more likely had a different outcome under the GDPR. This demonstrates a notable weakness within the PDPO as a functioning piece of legislation for protecting private data.

Interestingly, while the two regimes offer completely contrasting approaches to defining personal data, case law demonstrates that they have produced a similar functionality and actual working definition of personal data. In *Wu Kit Ping v Administrative Appeals Board,*[80] the subject had requested access to their medical records, including a report covering a complaint investigation they had instigated. Upon receiving a redacted copy they lodged a complaint with the Commissioner. The court upheld the Commissioner's findings that the subject is only entitled to a copy of information relating directly or indirectly to themselves, but that does not mean every document which may refer to them.[81] There is a need, as Cheung shows, for a significant biographical aspect and focus within the data to fall within the definition of personal data.[82] Similarly within the UK, in the case *Durant v Financial Services Authority*,[83] the complainant had requested access to information and received a redacted copy. The court stated that the mere mention of a name does not constitute personal data.[84] Nor does a subject have the right of access to a document which may contain their name.[85] Furthermore, the data controller has the right to redact information if it is not part of the requestor's personal data.[86] For data to become personal data, there is a need for it to be in 'a continuum of relevance or proximity to the data subject', with there being a specific focus on the data subject.[87] The outcomes of both these cases, while relying on different legal regimes and differing definitions of personal data, are similar, which raises interesting questions about the actual functionality of each regime in protecting individuals' data privacy. It would suggest that while on the surface, the PDPO seemingly offers less protection than the GDPR, in practice, at least in this specific area, it is functionally similar.

5. MEDIA AND DATA PROTECTION

Another aspect through which to functionally compare the two regimes is how the PDPO and GDPR balance the conflict between data protection and freedom of expression. A significant obstacle in data protection is the need to balance a person's right to privacy with freedom of expression– a perennial problem within human rights law. This has only become more pertinent in the internet age where, not only is there more data, but that data is more accessible and possible to spread quicker and further.[88] The internet era calls for greater protection, which is one of the reasons for the implementation of the GDPR in Europe. Therefore, a comparison of how the two jurisdictions provide mechanisms through which to balance this conflict offers an opportunity to further compare the functionality of the regimes.

5.1 UK Right To Privacy And Freedom Of Expression

The media has been pervasive in attempting to gain access to personal data – be that in the form of photographs, personal letters (for instance Meghan Markle's letters[89]), or more traditional forms of data such as documents and records– to substantiate sensationalised stories often framed within the argument of public interest. While data protection is important, it is equally important not to allow data protection to be used to stifle free press.[90] The UK GDPR attempts to afford a balance between an individual's data protection and freedom of expression by including a specific exemption for journalism, artistic or literary expression.[91] Before the introduction of the GDPR, there were numerous cases involving the publication of private information. For instance, *Campbell v MGN Ltd,*[92] whereby model Naomi Campbell sued over the publication of her attendance at narcotics anonymous alleging a breach of privacy. The court ruling

demonstrates the difficulty in striking a balance between freedom of expression and privacy. Lords Nicholls and Hoffman, dissenting, held that the covertly taken photos and publication did not amount to an intrusion of privacy. [93] However, the majority ruled that the publication of all materials in combination with the photos amounted to exceeding the balance between the right to privacy and freedom of expression. [94] Placing this in the context of data protection, it demonstrates that before the implementation of the GDPR, there was a weakness in the protection of people's private data, in this case, photographs. The GDPR set out far more stringent criteria than before.[95]

Two cases further demonstrate the importance of the need for strong data protection frameworks in the face of growing invasive technology. Firstly, The News International phone hacking scandal whereby it was revealed the paper had illegally accessed phone records. The subsequent Leveson inquiry stated that s. 32 of the DPA 1998 needed to have a narrower inception of the journalism exception.[96] It was recommended there should not be any exemption from DPPs 1, 2, 4, 6 and 8 to ensure that an individual's personal data is afforded proper protection. [97] These recommendations and the UK GDPR, however, remain to be seen how effective they will be in functionally protection people's data. The current case involving several celebrities against the Associated Newspapers[98] again centres on allegations of phone tapping and bugging, thus leading to the revealing of personal information in publications. It remains to be seen how the court will handle this case in light of the stricter stance taken by the UK GDPR, DPA and previous case law.

5.2 Hong Kong PDPO And Right To Privacy

Hong Kong has a similarly pervasive media who are, as Jojo Mo describes, intruding on privacy in search of ever more flashing and flamboyant news reporting.[99] As was already discussed earlier, the *Eastweek* case highlighted similar issues as to the *Campbell* case, whereby data in the form of photographs, were collected without consent and subsequently published. However, the court ruled that these were not to be deemed personal data, and consequently not a breach of DPP 1– collection of personal data by fair means. This is because the individuals photographed were never intended to be identified, and thus 'anonymised'. Through these two cases, it is apparent that both data protection regimes function differently. This is due to the glaring difference between how each case defines consent and what constitutes personal data. In the *Eastweek* case, by not intending to publish the identity of the women, the photographs are deemed not to be personal data. This distinction serves to seriously undermine personal privacy and protection over one's data, leaving the data protection regime open to abuse by the media. The Campbell case, on the other hand, was deemed to be a breach. This is because the public right to know is outweighed by Campbell's right to privacy and the combination of photographs and story meant there had been an intrusion of privacy. Hong Kong's Data Protection Ordinance provides news with a similar exemption as that of the DPA 1998. For instance, if there is a reasonable belief of public interest then any data processed and collected with the intention of publication is exempt from DPP 3 which outlines the use of personal data.[100] It is unsurprising therefore that in cases the balance often falls towards freedom of expression over personal data thus undermining data protection in comparison to the GDPR. Furthermore, functionally the two regimes are divergent in striking a balance between press freedom and privacy.

6. CONCLUSION

Hong Kong's data protection regime and the EU Directive 95/46 are extremely comparable in functionality and black-letter, with minor differences in definitions of personal data and exact operations. However, Hong Kong's data protection regime when compared against the comprehensive GDPR, does appear to be lacking in functionality with severe issues over consent, defining personal data and securing people's digital persona. By having such a strict and narrow definition of personal data, it is difficult for an individual to access any of the protections afforded to them by the PDPO once personal data has been misused. However, as demonstrated by the inclusion of provisions specifically targeting direct marketing and doxing, the PDPO is slowly providing greater protection. In some respects, the PDPO exists at the forefront of data protection, with specific doxing legislation being a notable absence form UK and EU data protection law.

There is a gradual convergence with the GDPR due to two main reasons. Firstly, to maintain its status as a financial hub its laws must be able to promote trust and a free-flowing market. If the data protection regime lacks this, Hong Kong's position is under threat due to the GDPR's transfer of data prohibition to territories without adequate protection. Equally, with public expectation demanding increased protection over data and privacy it is necessary that the legal regimes are able to promote and meet these demands. Secondly, Hong Kong is slowly evolving and reforming its PDPO as new technology forces adaptation by revealing specific weaknesses. In doing so the PDPO targets specific known issues making it in many ways more robust, and in the case of doxing being at the forefront of data protection developments. However, this method means there is an inherent inflexibility to it, making the data protection laws weak and vulnerable to rapidly developing technologies. The more flexible and broader in definition but comprehensive GDPR is, if one is to make a 'who-did-it-best' analysis, a better and stronger piece of legislation affording greater protection to the individual being rooted in the fundamental human right of privacy. Nonetheless, a comparison of court cases and

amendments shows that functionally the PDPO is converging with the GDPR, transforming into a more comprehensive piece of legislation as it works to enable Hong Kong's position as a financial hub.

---

[*] LLM International Environmental Law, Hourly-Paid Lecturer at Nottingham Law School. I am grateful for the guidance, teaching and encouragement from Prof. Janice Denoncourt.

[1] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD Publishing, 2002)

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1 [Hereinafter GDPR]

[3] Convention for the protection of individuals with regard to automatic processing of personal data [1981] ETS 108 [hereinafter Convention 108]

[4] OECD (n. 1) para. 7-14

[5] As amended by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419)

[6] Personal Data (Privacy) Ordinance (Cap. 486) 1995 (as amended in 2012 and 2021) [hereinafter PDPO]

[7] Gerhard Dannemann, 'Comparative law: Study of Similarities or Differences?' in Reimann, Mathias and Reinhard Zimmerman (ed.), *The Oxford Handbook of Comparative Law* (2nd edition, Oxford University Press, 2019) 413

[8] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281

[9] Ibid 391

[10] Ibid 413

[11] Ralf Michaels, 'The functional method of comparative law' in Reimann, Mathias, and Reinhard Zimmermann (eds), *The Oxford Handbook of Comparative Law* (Oxford University Press, 2006) 342

[12] Dannemann (n. 8) 394

[13] Geoffrey Samuel, *An Introduction to Comparative Law Theory and Method* (London, Hart Publishing, 2014) 67

[14] Ibid 65

[15] Mathias Siems, *Comparative Law* (3rd edition, Cambridge University Press, Cambridge 2022) 295

[16] Ibid 295

[17] Aleksander Grebieniow, 'Comparative Law by Uwe Kischel, Oxford: Oxford University Press, 2019. X + 960 pp. Hardcover: £150' (2020) 15(1) Asian Journal of Comparative Law 191, 193

[18] Uwe Kischel, *Comparative Law* (Oxford University Press, Oxford, 2019) 173

[19] Ibid 88-90

[20] Samuel (n. 13) 79

[21] Michaels (n. 11) 347

[22] Ibid 347

[23] Dannemann (n. 8) 407

[24] Siems (n. 13) 288

[25] Ibid 290

[26] Horatia Muir Watt, 'Globalisation and Comparative Law' in Reimann, Mathias and Reinhard Zimmerman (ed.), *The Oxford Handbook of Comparative Law* (2nd edition, Oxford University Press, 2019) 599

[27] Ibid 602
[28] Ibid 391-2
[29] Dannemann (n. 8) 397
[30] Watt (n. 20) 621
[31] Andrew Charlesworth, 'Implementing the European union data protection directive 1995 in UK law: The data protection act 1998' (1999) 16(3) Gov Inform Q 203, 206
[32] Samuel (n. 13) 81
[33] Ibid 82
[34] Ibid 96-7
[35] Ibid 97, 107
[36] Ibid 80
[37] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281
[38] Google Spain SL, Google Inc. v AEPD, Mario Costeka Gonzalez (Case C-131/12) [2014] ECLI:EU:C:2014:317
[39] Oxford English Dictionary Online, 'Dox' (3rd Edition Oxford University Press, March 2022) <https://www.oed.com/view/Entry/90792179?redirectedFrom=doxxing> accessed 12 June 2023.
[40]Kahon Chan,'Hong Kong privacy watchdog records 15 per cent jump in complaints after anti-doxxing law introduced' (South China Morning Post, 9 February 2023) <https://www.scmp.com/news/hong-kong/law-and-crime/article/3209680/hong-kong-privacy-watchdog-records-15-cent-jump-complaints-after-anti-doxxing-law-introduced> accessed 26 April 2023.
[41] PDPO (n. 7) schedule 1; Data Protection Act 2018 s.35-40; UK GDPR art. 5.
[42] Data Protection Act 2018 schedule 12; PDPO (n. 7) s. 5
[43] Data Protection Act 2018 schedule 13; PDPO (n. 7) s. 8
[44] Data Protection Act 2018 schedule 15
[45]Data Protection Act 2018 s.67
[46] Office of the Privacy Commissioner for Personal Data, 'Data Breach Notification' <https://www.pcpd.org.hk/english/enforcement/data_breach_notification/dbn.html> accessed 26 April 2023
[47] Gamvros, Anna and Yau Edward, 'Hong Kong's data privacy law reform may come in 2023' (Data Protection Report Norton Rose Fulbright, 6 Marcy 2023) <https://www.dataprotectionreport.com/2023/03/hong-kongs-data-privacy-law-reform-may-come-in-2023/> accessed 27 April 2023
[48] Privacy Commissioner, *Cathay Pacifc Airways Ltd and Hong Kong Dragon Airways Ltd* (Data Breach Incident report no. R19-15281, 2019)
[49] PDPO (n. 7) s. 64(1), (3)
[50] Ibid s. 64(3A), (3B)
[51] Ibid s.35J(5)(b)
[52] Office of the Privacy Commissioner for Personal Data, 'The Personal Data (Privacy) Ordinance' <https://www.pcpd.org.hk/english/data_privacy_law/ordinance_at_a_Glance/ordinance.html> accessed 26 April 2023
[53] Peter Lacos and Jennifer Boyse, 'GDPR and Hong King's PDPO: Are They So Different?' (Regulation Asia, 6 November 2018) <https://www.regulationasia.com/gdpr-and-hong-kongs-pdpo-are-they-so-different/#:~:text=GDPR%20defines%20personal%20data%20to,personal%20data%20for%20all%20purposes.> accessed 26 April 2023
[54] Anne S. Y. Cheung, 'An evaluation of personal data protection in Hong Kong Special Administrative Region (1995-2012)' (2013) 3(1) International Data Privacy Law 29, 29
[55] Office of the Privacy Commissioner for Personal Data, 'Eu General Data Protection Regulation (GDPR) <https://www.pcpd.org.hk/english/data_privacy_law/eu/eu.html> accessed 27 April 2023
[56] W. K. Hon, Julia Hörnle and Christopher Millard, 'Data protection jurisdiction and cloud computing - when are cloud users and providers subject to EU data protection law? The cloud of unknowing' (2012) 26(2-3) International review of law, computers & technology 129, 130-131

[57] Ibid 131
[58] GDPR (n. 2) art. 4(11)
[59] Michelle Goddard, 'The EU General Data Protection Regulation (GDPR): European Regulation that has a Global Impact' (2017) 59(6) International Journal of Market Research 703, 704
[60] PDPO (n. 7) s. 35E
[61] [2008] 5 HKC 229
[62] Ibid para. 41
[63] Ibid para. 42
[64] [2000] 1 HKC 692
[65] Jojo Y. C., Mo, 'Are data protection laws sufficient for privacy intrusions? The case in Hong Kong' (2014) 30(4) The computer law and security report 429, 431
[66] Ibid 431
[67] Privacy Commissioner, *The Collection and Use of Personal Data of Members under the Octopus Rewards Programme run by Octopus Rewards Limited* (Report No. R10-9866, October 2010) para 16.2
[68] Cheung (n. 42) 29
[69] PDPO (n. 7) s. 35C, 35E
[70] Nuala O'Connor, Alethea Lange and Ali Lange, 'Privacy in the Digital Age' (2015) Great Decisions 17, 18
[71] Ibid 18
[72] Ibid 18
[73] PDPO (n. 7) s. 64(1)
[74] Marija Boban, 'Digital Single Market And Eu Data Protection Reform With Regard To The Processing Of Personal Data As The Challenge Of The Modern World' [2016] Varazdin Development and Entrepreneurship Agency (VADEA) 191, 198
[75] Data Protection Act 2018 s.3(2)
[76] PDPO (n. 7) s. 64(1)
[77] Ibid s. 2
[78] Cheung (n. 42) 432
[79] Octopus Report (n. 57) para 16.3
[80] [2007] 5 HKC 450
[81] Ibid para. 32
[82] Cheung (n.42) 432
[83] [2003] EWCA Civ 1746
[84] Ibid para. 28
[85] Ibid para. 30
[86] Ibid para. 65
[87] Ibid para. 28
[88] Andreas Wiebe, 'Data protection and the internet: irreconcilable opposites? The EU Data Protection Reform Package and CJEU case law' (2014) 10(1) Journal of Intellectual Property Law & Practice 64, 65
[89] HRH Duchess of Sussex v Associated Newspapers Ltd [2020] EWHC 2160
[90] Nani Jansen Reventlow, 'Can the GDPR and Freedom of Expression Coexist?' (2020) 114 AJIL Unbound 31, 31 <https://www.cambridge.org/core/article/can-the-gdpr-and-freedom-of-expression-coexist/C8C5B4F0BFF87B9CAD78ED4BDDF27BBC> accessed 26 April 2023
[91] GDPR (n. 2) art. 85(2)
[92] [2004] UKHL 22
[93] Ibid para. 34
[94] Ibid para. 124
[95] Data Protection Act 1998 s.32
[96] Lord Justice Levenson, An Inquiry Into the Culture, Practices and Ethics of the Press (TSO(The Stationery Office) 2012) recommendations para 48
[97] Ibid recommendations para 49

[98] Minelle Bethany, 'Prince Harry v Associated Newspapers: Everything you need to know about the Duke of Sussex's latest court case' (Sky News, 27 March 2023) <https://news.sky.com/story/prince-harry-v-associated-newspapers-everything-you-need-to-know-about-the-duke-of-sussexs-latest-court-case-12839560> accessed 26 April 2023

[99] Mo (n. 53) 429

[100] PDPO (n. 7) s. 61

AI TIPPING POINT: AN ANALYSIS OF THE EU & CHINA'S REGULATORY APPROACH

SID ALI BOUTELLIS*

Abstract

This paper provides a comparative analysis of AI regulation in the European Union (EU) and China, two major players in the global AI landscape. The EU has adopted a proactive approach with its comprehensive AI Act, emphasizing ethical principles and fundamental rights, aiming to strike a balance between innovation and societal safeguards. In contrast, China prioritizes innovation and adapted a more flexible approach, particularly with the implementation of the Development Plan for Next Generation AI, whilst maintaining a strict policy surrounding government supervision and national security. This article explores the underlying factors driving these divergent approaches, challenges in implementation, and their broader implications for AI governance. Mainly focusing on how the EU implements a stringent AI-centric legislation across its various jurisdictions and how China aims to strike a balance between innovation whilst minimizing the security risks inherent to AI.

INTRODUCTION

In order to best understand the legal implications and ramifications regarding Artificial Intelligence (AI) for businesses and societies in general, it is necessary to go through a scientific prelude to better grasp this technology. The concept of AI has been associated with a plethora of definitions. A rather simple and intuitive way to define it is: 'The art of creating machines that perform functions (requiring) intelligence when performed by people'.[1] Although it is tempting to delve into the philosophical and legal interpretations of the words: 'art', 'intelligence', and 'machines'; this article rather focuses on explaining the functional aspects of AI. By taking a practical approach to defining AI, it is not possible to shed light on the complex applications of this technology without touching on relevant computer science principles such as Machine Learning, Large Language Models (LLMs), or Black Box AI.

Today's digital age is fuelled by data and AI is the engine that burns this fuel. Not different from the industrial revolution, when an engine could be an integral part of a car or

alternatively a train, AI's multi-disciplinary nature works in the same way. It is a field within computer science and engineering that focuses on leveraging very large sets of data to power various systems that perform human-like cognitive functions at record speed. These systems have a range of applications that include but are not limited to: Natural Language Processing (NLP) models, Robotics, Search Algorithms, Expert Systems, and the list goes on. These scientific discoveries are then implemented across all disciplines establishing AI's dominant presence in commercial, public, and industrial sectors. To understand why these computationally advanced systems are indispensable, it is necessary to have an overview of their inner workings and gain some insight on the major techniques being used today.

Machine Learning

At the top of the list sits Machine Learning (ML) due to its inherent ability to autonomously process large data sets while distinguishing subtle patterns allowing for a rational and logical manifestation of AI in action. ML is a key subset of AI that enables systems to learn and make predictions or decisions from data. The field is broadly categorized into three primary types: supervised learning, where models are trained on labelled data; unsupervised learning, which identifies patterns in unlabelled data; and reinforcement learning, where agents learn through interactions with their environment.[2]

Many AI agents, including those used in recommendation systems, natural language processing, and image recognition, are powered by machine learning algorithms.[3] These agents learn patterns and information from data to make informed decisions or provide intelligent responses. The nomenclature of the ML subcategories does not reflect the level of human intervention but rather the nature of data fed into the system and whether input/output mapping exists to limit the range of potential solutions along with the level of automation involved in the statistical analysis.[4]

Due to its foundational usage of neural networks, ML is present in various systems that stem from AI. A visual way of looking at this is by considering AI as a Tier 1 computer science method then ML would be Tier 2.[5] Neural Networks on the other hand are not a system that stems from AI. A neural network is a mathematical model composed of layers of interconnected nodes, often referred to as neurons or artificial neurons, designed to process and learn from data.[6] It is designed to mimic the human brain's neurons and is composed of an input layer that receives the data to be processed, an output layer that produces the final result

or prediction, and hidden layers in between in charge of processing the information from the input layer feeding into the output layer.[7]

The importance of defining neural networks in this context is to paint a picture of how the data travels through the cycles and the variance in complexity. The more complex a system the more layers exist in the neural network which leads to increased difficulty in understanding the outcome achieved by the system as it becomes impossible to find a logical link between the input and output obtained.[8] Those using these systems may achieve better results but it will occur at the detriment of transparency and this is what prompted an urge for ethical considerations.

Black Box AI

The idea of "Black Box AI" has recently gained in popularity and is present in most academic articles involving AI, particularly those targeting applications within education and healthcare. Black Box AI is not a different computational subset of AI but rather refers to a state produced by exceedingly complex algorithms as was earlier described with neural networks.

By applying advanced statistical models that are mathematically abstract yet optimize computational efficiency, these systems can obtain impressive results at low costs.[9] Nevertheless, the increase in efficiency comes at the hefty price of transparency and interpretability. The abstract computations involved through the countless layers of neural networks lack a causal link between the input provided and the output generated.[10] In most cases, human intervention is incapable of identifying the reasons behind the produced outcome. The lack of opacity in these systems coupled with the inherent bias generated through statistical analysis is a perfect illustration of the risks associated with AI and the necessity of human intervention in order to promote fairness in a democratic society.[11]

The best way to understand the significance in practical and regulatory challenges that come with Black Box AI is by virtue of an example. As aforementioned, education and healthcare have become systematically concerning when discussing the ethics of AI. When discussing healthcare, it stems naturally that 'one fundamental barrier' to opportunities with AI is 'low levels of public trust' and, in the health context in particular, that practitioner (clinician) distrust is more prominent than in other sectors.[12] Putting this into context, AI could jeopardise the physician–patient relationship, for example the "black box" phenomenon could

prevent the doctor from providing clear information to patients.[13] The clinician must have confidence that the decision support tool will do what it is supposed to and not cause harm for which they may be legally responsible.[14] For clinicians then, trustworthy AI/CDSS should be an accurate tool, whose design, engineering and operation ensures they generate positive outcomes, and mitigates potentially harmful ones.[15] Therefore, it follows naturally that the inherent opacity of Black Box AI will always be a major concern with potential for legal liability in healthcare.

GOAL OF THIS ARTICLE

Although the technical introduction may seem dense for some readers, it serves as a beacon for when we delve into the regulatory landscape of AI in EU and China. Defining Machine Learning and Black Box AI will be crucial for providing illustrative guidance when discussing regulatory and ethical challenges.

Having established a relationship between some of the modern AI use-cases and their underlying functionality, it is now possible to discuss the current regulatory approach taken by two jurisdictions highly motivated towards winning the global race in AI innovation: EU and China. By analysing how these two regulatory bodies have addressed the rapid AI evolution and assessed the public impact, it is possible to provide some guidance on how organizations should adjust their technology adoption strategy, governance culture, and risk mitigation in relation to AI-driven initiatives.

The EU's Approach to AI Regulation

In the context of the European Union (EU), businesses either headquartered within its jurisdiction or engaged in commercial activities therein face the intricate regulatory landscape governed by four principal legislative frameworks. These regulatory pillars encompass the General Data Protection Regulation (GDPR), the EU AI Act, the AI Liability Directive, and the Updated Product Liability Directive. These legislative instruments collectively delineate the legal boundaries and obligations that companies operating in the EU must navigate and comply with, addressing critical aspects ranging from data protection and artificial intelligence governance to liability frameworks in the ever-evolving digital and technological landscape. This section provides an overview of the regulatory framework that is paramount for businesses

within the EU, emphasizing the multifaceted nature of compliance requirements spanning data privacy, the emergence of new technologies, and the strategies necessary for AI liability mitigation.

GDPR

According to Ben Welford, the General Data Protection Regulation (GDPR) is the toughest privacy and security law in the world.[16] Compliance requirements under the GDPR can vary based on industry and the nature of data processing activities. While the GDPR sets universal data protection principles and rights, industries may have additional regulations specific to their sector. Variations may arise from the types of data handled, the purposes of processing, organizational size, geographical reach, and sector-specific laws. Organizations need to carefully assess their data processing operations, understand any industry-specific requirements, and ensure full compliance with both the GDPR and relevant sector-specific regulations.

An item of critical importance is that all the governance controls that have been put in place to adhere to GDPR must be leveraged to develop a robust AI compliance mechanism. An example showcasing the benefit of building AI regulation on top of GDPR mandates is shown in Recital 7 of the AI Act 2021,[17] which requires that biometric data be interpreted consistently with the principles depicted in GDPR.[18] In addition to the similarities in scope between AI and GDPR regulations, there is also significant overlap in terms of risk mitigation and sanctions between the two mandates.[19] Organizations having already gone through the hurdles of compliance with GDPR, can benefit from the process and apply a similar approach towards AI compliance. These measures include robust data encryption protocols, comprehensive privacy impact assessments, continuous staff training programs, strict access controls, and transparent data processing documentation, all aimed at ensuring the lawful and responsible handling of personal data.[20]

It naturally follows that a stringent regulation like GDPR hinders the ability for companies to innovate and promote an aggressive agenda towards releasing AI technologies. Currently, the inherent legal risk in European jurisdictions requires careful monitoring of new laws and an assessment of potential costs in the event of liability. Given the accountability duties under GDPR, defending a claim for AI-based decision-making will prove expensive and the organization can be vulnerable from several fronts. Additionally, there are a number of

other legal channels that can be leveraged for litigious purposes for which AI solution providers must assess the risk. A claim can be brought in Tort under product liability as will be discussed later, infringement of GDPR mandates, or even human rights as a potential breach of Article 16 TFEU and similarly Article 8 ECHR. And these are only a few examples of mediums through which plaintiffs can bring a claim which demonstrates the wide exposure for pioneers in AI service provision.

Compliance with GDPR will open the door to alleviate the burden of compliance in AI-specific legislation because it was designed with technologies like AI in mind.[21] Nevertheless, the specific provisions drafted in the GDPR that target emerging technologies are vague and open-ended.[22] The lack of precision in the law today is not surprising and can be attributed to the fact that developments in the computer science space are happening at an unexpectedly high velocity. Which is a clear indicator for the need of reform in the regulatory framework overseeing AI.

EU AI Act

In order to complement and fill the gaps that are not covered by GDPR, the European Commission (EC) proposed their first official draft of the EU AI Act in April 2021.[23] The Council of the European Union (CEU) then adopted its own common position on the AI Act in December 2022.[24] On June 14, 2023, the EU Parliament created a third version of the legislation by adopting a series of amendments to the EC Proposal.[25] Finally after negotiations between the three parties were complete, Parliament adopted the Act in March 2024 and the Council followed with its approval in 2024.[26] The Act was then published in the official Journal of the European Union on 12 July 2024[27] and came into force on August 1st 2024.[28] A distinguishing characteristic of the EU AI Act is that although it came in force in August of 2024 as a regulatory document, it shall apply from 2 August 2026.[29] There are however a number of articles that will apply gradually starting as early as 2 February 2025 up until 2 August 2027 according to Article 113 of the regulatory text. This means that the legislation will be binding on member states piecemeal, giving nations the opportunity to adjust their domestic initiatives in accordance with which chapters will apply first. Chapters I and II touching on the general provisions of the Act as well as the prohibited AI practices are most crucial and therefore applied first on 2 February 2025. The bulk of the regulation focuses on High-Risk AI systems and how providers must adapt to showcase safety and transparency

within their systems. Most of these rules will apply 12 months after the legislation first came into force in August 2024.

The phased-out approach for the EU AI Act to become applicable, raises the question of adequacy given the current pace of AI development. Prima facie, the estimated three-year timeline is far from promising. It is possible for legislation to undergo significant changes during this time enabling adjustment to current regulatory needs, however, the horizontal approach for regulation lacks versatility, particularly for multisector moderation. As perceived today, the processes put in place by the EC, CEU, and EU Parliament are lengthy and repetitive. Having such a slow approach towards creating AI-centric legislation will give the public the lasting impression that the law is constantly lagging relative to technology. Similarly, the strict requirements imposed on High-Risk AI systems may create a burden on the judicial bodies from companies aiming to show that their solution does not present a high risk. Those who are successful will have expended a large portion of their resources in making this case; an amount that will be negligeable compared to what High-Risk system providers will have to pay to abide by the legislation. The strict requirement will encourage international? companies to seek alternative jurisdictions for AI solutions and local companies will have to stifle their development. The results could be catastrophic for member states' economies and the position of the EU in the AI race for innovation.

On the other hand, the prudent approach taken by the EU can set the global pace towards the implementation of AI-centric laws that could be embraced at a global scale. Having laws that put safety and humans at the centre can strongly motivate the global regulatory ideology. The best way to visualize the impact of AI systems on consumers is by analysing the four main categories depicted in the Act: Unacceptable Risk, High-Risk, Limited Risk, and Minimal Risk systems.[30] Of these, the most relevant and potentially concerning to organizations are the unacceptable and high-risk systems, being mindful that the bulk of the legislation aims to cover high risk AI systems. The unacceptable risk systems are those that have the potential to cause significant harm to persons or vulnerable groups like children, in addition to social scoring and real-time remote biometric identification systems by means of example.[31] The High-Risk systems are those that operate on critical infrastructure like education, transport, or healthcare.[32] Individuals should maintain awareness of the limited and minimal risk systems, nevertheless, as the ramifications in the long run have not been identified. As user adoption

increases in the AI space, the risks will grow, and given the slow pace of legislation, the public must create safeguards they can enforce at their level, whether it is through associations, awareness groups, or even social media campaigns.

Operating an intelligent system, as the definition of AI suggests, will naturally provide it with a degree of autonomy. Decision-making driven by AI is strongly based on the data provided, while the processing power quickly identifies various patterns. This mechanism is prone to bias. For instance, a 2019 study shows that less than 15% of STEM professionals are women.[33] Applying the models employed by AI such as unsupervised ML which is heavily reliant on input data, can possibly infer that men are better suited for STEM roles. Even if limits and thresholds are put in place to promote a fair outcome, a complex AI decision-making system in the field of recruitment can very possibly display data-driven bias. The STEM recruitment theoretical example aligns with NIST's view about AI bias being a particular concern, however, the bias stems from systemic biases that then propagate into the human population that is finally inducing computational bias.[34] Given the nature of the beast, regulators need to be wary about taking computational results without putting them through the societal scrutiny that humans are subjected to.

Alternatively, when deployed properly with appropriate safeguards, AI will undoubtedly provide significant benefits to society by processing very large data sets and identifying subtle patterns, such as predicting future seismic events based on past and current data and save countless lives in a time where seismic events are increasingly frequent at high magnitudes.[35] Increasing trust in AI will prompt growth and innovation, but in order to do so we must identify the scope of liability. Margit Sutrop said that 'Public trust in new technologies also depends on the behaviour of scientists and developers, as well as the public understanding of science and acceptance of the applications of new scientific developments.[36] This sparks the debate as to how the public and organizations can place trust in an entity that is constantly changing and lacking in transparency. If things go terribly wrong, who will bear the burden of the blame? Bryson is clear on this point: "Like any other manufactured product, either the manufacturer or the owner/operator must be accountable for any damage it causes. Otherwise, malicious actors will attempt to evade liability for the software systems they create by blaming the system's characteristics such as autonomy or consciousness".[37]

In conclusion, the EU AI Act introduces a stringent regulatory landscape, emphasizing the gravity of compliance for organizations operating within its jurisdiction. Similar to GDPR, the potential financial repercussions are substantial. Noncompliance with the AI Act's prohibitions, as outlined in Article 5, exposes entities to formidable administrative fines, reaching a maximum of 35,000,000 EUR or, in the case of an undertaking, an imposing penalty of up to 7% of their total global annual turnover from the preceding financial year, whichever is higher.[38] The penalties for non-compliance are clearly defined in Article 99 of the EU AI Act and must be carefully reviewed. These substantial sanctions underscore the critical imperative for organizations to diligently adhere to the AI Act's provisions. Failure to do so not only poses a financial risk but also raises significant legal and reputational consequences, emphasizing the pivotal role of compliance in navigating the complex AI regulatory landscape of the European Union.

AI Liability Directive

The EU AI Liability directive was submitted in 2022 alongside the EU AI Act to navigate through the impracticalities of civil liability laws in context.[39] It is indispensable in the contemporary landscape of artificial intelligence (AI) due to several compelling reasons. First and foremost, AI systems, notably advanced machine learning models, often exhibit intricacy and opacity in their decision-making processes, rendering the establishment of liability and responsibility a formidable challenge.[40] Additionally, existing legal frameworks may inadequately address the unique complexities of AI technologies, including their autonomous operation and evolving nature.[41] The directive fills this regulatory void by providing a clear and modernized framework for attributing liability in AI-related cases, thereby safeguarding the interests of individuals and entities that may suffer harm. Moreover, it serves as a catalyst for responsible AI development, incentivizing developers and organizations to prioritize safety and transparency in their AI systems, knowing they can be held liable for any resulting harm. Furthermore, the directive contributes to the harmonization of AI liability rules across the European Union, ensuring consistency and legal clarity in an increasingly interconnected European market. Lastly, by addressing liability concerns, the directive fosters consumer confidence in AI technologies as they become an integral part of daily life. In essence, the EU AI Liability Directive plays a pivotal role in navigating the intricate legal landscape of AI, offering protection, accountability, and regulatory cohesion in an era of rapid AI advancement.

Underpinning the EU AI Liability Directive is its legal foundation in Article 114 of the Treaty on the Functioning of the European Union (TFEU), a provision aimed at ensuring the seamless operation of the internal market.[42] This directive is strategically designed to address two pivotal concerns integral to the evolving AI landscape. Firstly, it focuses on the accessibility of evidence for parties adversely affected by AI-related incidents, streamlining the process of establishing liability. Secondly, the directive introduces a rebuttable presumption emphasizing a causal link between the failure of duty of care and the harm incurred due to AI systems.[43] While these concepts are legally intricate and demand thorough examination, their central objective is unequivocal: to broaden the scope of "products" within the legal framework, encompassing AI systems. This expansion reflects a proactive approach to adapt liability principles to the burgeoning AI sphere, aligning legal norms with technological advancements and ensuring equitable recourse for all stakeholders.

Furthermore, as organizations navigate the complexities of the EU AI Liability Directive, a prudent approach is to consider it in conjunction with the EU AI Act. Notably, numerous definitions within the directive align with those in the AI Act, a strategic move to maintain consistency and coherence in AI-related regulations. This harmonization significantly broadens the scope of liability, encompassing a wide array of AI systems subject to the AI Act's provisions. Consequently, organizations are poised to encounter multifaceted legal liability exposures, necessitating a comprehensive strategy to mitigate risks on various fronts. This entails fostering a governance-centric corporate culture that places a premium on compliance, accountability, and ethical AI practices. Equally vital is the emphasis on meticulous documentation to substantiate adherence to regulatory frameworks. Conversely, consumers, while gaining the ability to pursue claims from diverse angles, must be cognizant of the rigorous demands associated with satisfying the burden of proof. The convergence of these dynamics underscores the critical importance of proactive and robust organizational practices in navigating the evolving landscape of AI liability within the European Union.

Updated Product Liability Directive

The "updated product liability directive" serves a vital purpose within the European Union, primarily geared towards ensuring the seamless functioning of the internal market in the face of evolving technology.[44] It achieves this by meticulously adapting existing legislation to

accommodate the complexities posed by products in the digital age. Significantly, this directive responds to transformative shifts that have occurred since the inception of the Product Liability Directive (PLD) in 1985. Notably, there has been a substantial uptick in consumers directly acquiring products from non-EU countries, underscoring the need for an evolved approach that extends beyond traditional fault-based liability. This shift is further exemplified by the expanded scale of operations by manufacturers, necessitating a more robust regulatory framework. Crucially, the directive addresses this requirement by broadening the scope of what constitutes a "product" within the PLD, explicitly encompassing AI systems.[45] This strategic adaptation reflects a forward-looking commitment to aligning legal norms with the dynamic landscape of technological innovation while fostering harmonization and clarity in product liability standards within the EU market.

To understand the impact of the updates to the PLD from an AI-centric perspective, it is necessary to look at the specific guidelines of the directive, particularly Article 6 of the Updated PLD with respect to “defectiveness”. The updated scope of a defective product now encompasses the capability of systems to undergo continuous learning post-development, in addition to stringent safety-related cybersecurity requirements. Consequently, manufacturers can still be liable even after the product has left their control.[46] These changes are critical for all organizations in the digital sector regardless of their implication in AI systems. In expanding the scope of the PDL, many organizations who offer digital services need to reassess their risk mitigation frameworks to include potential tortious liability by virtue of the new legislation. Additionally, non-EU product providers and consumers who directly acquire these products need to be mindful of the requirement for an EU importer or manufacturer who serves as an intermediary for distribution, resulting in additional cost for the suppliers and subsequently the consumers.

While the updated product liability directive seemingly favours consumers by expanding the scope of liability, it also incorporates provisions that grant manufacturers certain exemptions from liability, thereby shifting the burden of proof onto them. A noteworthy consideration within this context pertains to Article 10 (1) (e), which allows for the exclusion of liability based on a lack of knowledge considering the prevailing state of scientific and technical knowledge at the time. This provision introduces an intriguing dimension, especially in light of the growing complexity of emerging technologies and the evolving landscape of

knowledge. Manufacturers are likely to find the defence under Article 10 (1) (e) particularly appealing, and as a consequence, courts will face the intricate task of striking a delicate balance between the evolving state of knowledge and the overarching duty of care, ensuring equitable outcomes within the framework of product liability legislation.

KEY TAKEAWAYS FROM EUROPE

In summary, Europe has set a global benchmark for data regulation through the successful implementation of GDPR in 2018 and seeks to extend this leadership to the realm of artificial intelligence through the EU AI Act. The outcome of Europe's ambitions in AI regulation hinges on the region's ability to foster the technical growth of AI systems while concurrently nurturing economic prosperity. This aspiration, however, confronts formidable challenges, notably competition from innovation-driven nations like the United States, which prioritize technological advancement over stringent regulation. Europe's current strategy revolves around the adoption of rigorous auditing requirements, a move that, while enhancing accountability, also bears the potential to inhibit innovation and potentially create disparities in the global AI landscape.

All this to say, that vigilance is paramount as the legislative landscape evolves. Businesses should adopt adaptive practices that can keep pace with the velocity of legal and technological advancements. This necessitates substantial investments in robust cybersecurity infrastructure to safeguard against AI-based threats and mitigate the risk of hefty legal penalties. Equally critical is prioritizing information governance to establish precise control over data assets. Finally, AI governance should strike a balanced equilibrium between legal risk-mitigation and fostering innovation. If organizations establish a strong foundation in cybersecurity and information governance, they can pivot toward prioritizing innovation, confident in their ability to swiftly adapt to new legislation as it unfolds. These key takeaways underscore the intricate interplay between regulation, innovation, and strategic foresight in Europe's evolving approach to AI governance.

CHINA’S APPROACH TO AI REGULATION –

China is grappling with the formidable challenges posed by the rapid advancement and widespread integration of AI and the swift digitalization across various facets of society and

the economy. This surge has given rise to concerns regarding privacy, personal information protection, and data security for both individuals and businesses. The escalating volume of legal disputes related to AI and data has prompted legislative and judicial responses. Notable cases, such as the record-breaking fine imposed on Alibaba for antitrust violations and a court ruling against Ctrip for biased algorithms, have garnered substantial media attention and catalysed the emergence of laws and regulations in China, focusing on data security, personal information protection, and AI.[47] China's legal framework encompasses a range of statutes, including the Criminal Law, Civil Code, Cybersecurity Law,[48] Data Security Law,[49] and the landmark Personal Information Protection Law,[50] which collectively establish rules for data handling and privacy protection. Additionally, the nation has embarked on a multi-step strategy outlined in the 2017 Development Plan for the Next Generation AI, setting ambitious goals for AI legislation and governance by 2030.

Similar to our examination of the European Union's regulatory framework in this article, a critical examination of China's legislative foundations is imperative for a holistic understanding of their approach to AI regulation. In shaping their strategy for governing artificial intelligence, China relies on a multifaceted legal framework encompassing pivotal instruments such as the Personal Information Protection Law (PIPL), the Cybersecurity Law, and the forward-looking Development Plan for the Next Generation AI and will be highlighted in this article. It is noteworthy that this compilation of pertinent legislation is not exhaustive; factors within the Criminal Law, the Civil Code, and Antitrust laws also play integral roles. By conducting this comprehensive analysis, our objective is to unravel the intricacies of China's AI regulatory landscape and discern its significance, both on a domestic scale and within the broader global context, offering a comparative perspective with the European Union.

Personal Information Protection Law (PIPL)

One of the main reasons for covering the Personal Information Protection Law (PIPL) in China relative to the EU approach in AI regulation is that it shares several notable similarities with the European Union's General Data Protection Regulation (GDPR).[51] Both laws have extraterritorial applicability, extending their reach beyond their respective regions to regulate the processing of personal data concerning individuals within their territories. They establish similar roles, with data controllers and data processors having specific responsibilities, and they emphasize the importance of lawful bases for data processing, including consent,

contractual necessity, and legal obligations. [52] Additionally, both laws impose strict requirements for data breach notifications, safeguard the rights of data subjects, regulate cross-border data transfers, address automated decision-making to prevent discrimination, and outline penalties for non-compliance.

Despite these parallels, the PIPL and GDPR also exhibit differences, such as variations in the scope of cross-border transfer restrictions, unique requirements, and some nuanced distinctions in their respective provisions.[53] Organizations operating within both China and the European Union must carefully navigate these similarities and differences to ensure full compliance with both regulatory frameworks, thereby safeguarding individuals' data privacy in these regions.

To illustrate the development of regulatory principles within emerging technologies in China we take a slight tangent to mention blockchain service nodes. The technical nuances are not important for this context but the method of operation of these nodes from a computer science perspective is similar to convolutional neural networks (CNN), a principle mainly used in ML to train models by using images as input. In the realm of blockchain technology, a novel method and device have been devised to address a pressing technical challenge within alliance chain networks—namely, the protection of user privacy data from inadvertent exposure by blockchain service nodes. [54] This innovation hinges on the incorporation of a certificate authorization server (CA) certificate into communication requests, coupled with the prior configuration of a trust list for CAs. This ingenious approach enables the determination of whether a connection should be established with the service node, effectively curtailing unauthorized access. Consequently, this solution serves as a robust countermeasure against data leakage, substantially bolstering the overall security posture of alliance chain networks.[55]

This development carries significant implications, potentially simplifying the patenting process for inventions akin to the aforementioned blockchain safeguard. Such progressive changes could incentivize further innovation and investment in these domains within China's burgeoning technology landscape and they could not have been achieved without maintaining the core principles of PIPL in foresight.

The comparison between China's Personal Information Protection Law (PIPL) and the European Union's General Data Protection Regulation (GDPR) highlights significant

regulatory parallels, particularly in the context of AI and data privacy, emphasizing the importance of protecting individuals' data privacy on a global scale. The innovative application of PIPL principles to emerging technologies like blockchain service nodes reflects China's adaptability and fosters an environment conducive to innovation and patenting, showcasing the enduring influence of PIPL on China's AI regulation and its broader implications for businesses and technological advancements in the nation.

Cybersecurity Law

China's Cybersecurity Law, enacted in June 2017 and subsequently revised in December 2020, stands as a cornerstone in China's evolving digital landscape and its broader strategy to safeguard national cybersecurity. This comprehensive legislation, often regarded as one of the world's most stringent cybersecurity frameworks, serves a dual purpose: to bolster the protection of critical information infrastructure and to regulate the conduct of various digital stakeholders, including network operators, service providers, and data processors. Thus, AI systems in their nature fall within the governance framework of this legislation.

Embedded within the law are provisions that address data protection, cross-border data transfers, threat response mechanisms, and stringent cybersecurity assessments. Understanding the multifaceted dimensions and implications of China's Cybersecurity Law is crucial in comprehending the evolving cybersecurity landscape within the nation and its impact on businesses, data privacy, and international digital relations. Given the inherent security risk that AI systems can create in a country as populous as China, the control over systems susceptible of generating misinformation will likely be very strict. It is therefore imperative for businesses to assess whether their systems can be used in a manner that triggers misinformation campaigns and one way of limiting this to avoid integration with mass diffusion platforms like social media.

The growing concerns of using AI as a means to disrupt national security is at a high point and it is important for businesses to acknowledge this threat. The Cybersecurity Law restrictions will be a hurdle that needs overcoming by AI service providers even with proper business practices and enhanced safeguards in place.

Development Plan for the Next Generation AI

China's Ministry of Science and Technology (MOST) announced on March 9, 2020, the establishment of four new "National New Generation Artificial Intelligence Innovation and Development Pilot Zones" (hereafter referred to as "AI pilot zones"). These zones were officially approved by MOST and are located in the cities of Chengdu, Chongqing, Jinan, and Xi'an, further expanding the existing network of national AI pilot zones, which previously encompassed Beijing, Shanghai, Hangzhou, Hefei, Shenzhen, Tianjin, and Deqing County in Zhejiang Province, established in 2019. Remarkably, MOST has ambitious plans to establish approximately 20 AI pilot zones by 2023, as outlined in a notice issued in August 2019.[56] The primary objective of these AI pilot zones, as articulated by MOST, is to foster the continued growth of China's AI industry in cities where it has already firmly established itself. In return for their designation, both the central and local levels of the Chinese government extend various benefits to these AI pilot zones, including financial support and favourable local regulations. Consequently, these zones are expected to channel their efforts toward implementing AI applications that yield tangible economic, social, environmental, or other advantages to their respective regions.[57]

Despite the seemingly flexible stance that China has taken to promote innovation in the AI sector, their approach to AI regulation from a legal perspective showcases a proactive and comprehensive strategy aimed at governing this rapidly evolving technological landscape. One striking example of China's stringent stance is the recent draft proposal known as the "Measures for the Management of Generative Artificial Intelligence Services." Remarkably, this legal document is specifically tailored to address Generative AI, a technology that gained prominence only towards the end of 2022.[58] China has not hesitated to establish a legal framework addressing various facets of AI, as exemplified by the Personal Information Protection Law, Data Security Law, and Cybersecurity Law, each of which tackles distinct aspects of AI development, deployment, and interaction.[59]

China’s approach to regulation embodies a commitment to promoting accountability, transparency, and ethical use of AI while prohibiting misinformation and any attempts at subverting state authority, as evidenced in Article 4 of the draft "Measures for the Management of Generative Artificial Intelligence Services." Moreover, these regulations explicitly forbid discrimination on various grounds, ranging from race and ethnicity to religious belief and profession. Article 10 underscores the importance of preventing users from becoming

excessively reliant on or addicted to AI-generated content, highlighting China's forward-thinking and regulatory preparedness in addressing potential societal challenges associated with AI.

A prime example of "Regulations for the Promotion of the Development of the Artificial Intelligence Industry" in action, which also serves as part of the “Development Plan for Next Generation AI”, is the application of these laws in both the Shanghai Municipality[60] and the Shenzhen Special Economic Zone.[61] These regulations provide a high-level governance framework for AI while allowing for detailed implementation to be handled at the municipal level. Notably, these local legislations complement the broader national laws, such as the Personal Information Protection Law, Data Security Law, and Cybersecurity Law, which are expected to fill in the specifics of AI regulation. While these two local regulations share similar objectives, they target different subsets of AI sectors. For example, Shanghai’s AI advancement is targeted towards the improvement of scientific education resources ((科教资源), application scene (应用场景), Big Data (海量数据), and openness (开放).[62] Alternatively, Shenzen’s focus lies within R&D capacity, high concentration of high-end talent, complete production chain (产业链完整).[63]

To further illustrate the impact of Chinese legislation with respect to AI, two landmark cases must be analysed: Beijing Film Law Firm v Baidu Netcom Technology Co Ltd[64] along with Shenzhen Tencent Computer System Co Ltd v Shanghai Yingxun Technology Co.[65] One thing to note before going into a summary of the cases is that both courts in charge of delivering the verdicts were located in Beijing and Shenzhen respectively, additionally, both municipalities are part of the national AI pilot zones.

In the Baidu case, a Beijing law firm published an article on legal and judicial trends related to the film and television entertainment industry, which contained visual graphs and written analysis. The defendant, Baidu Netcom Technology Co Ltd, republished this article without permission. The court found that the visual graphs generated by software upon user input were not copyrightable because they lacked tangible originality, and similar graphs would result from similar data and software usage. Regarding the written analysis, although it displayed a degree of originality, the court ruled that it was not copyrightable because it was

created by software and did not reflect the original expression of a natural person's idea and emotion. However, the court did recognize the copyrightability of the written texts in the article, as they were independently created by the plaintiff. Baidu was held liable for copyright infringement and ordered to pay damages and publish a public apology.[66]

In the Tencent Dreamwriter case, the plaintiff had published a financial report, the creation of which was attributed to an AI software known as Dreamwriter. The defendant, as part of a marketing strategy, reproduced and published this report. The court, in contrast to the Baidu case, did not centre its analysis on whether the creator was a "natural" or "non-natural" entity. Instead, it focused on the article's inherent originality, emphasizing that it bore the marks of personalized choices and the skills exercised by a "creative team" throughout the entire creative process.[67]This distinctive approach led the court to conclude that the article was indeed copyrightable under Chinese intellectual property law. Consequently, the defendant was found liable for copyright infringement, resulting in the award of damages and a requirement for a public apology.

These cases underscored a human-centric perspective, rejecting the notion of AI machines possessing copyright interests while underscoring the paramount significance of originality in determining copyright eligibility. Notably, the key variance in the interpretation of the law between the two cases, as emphasized by Wengwei Li, was that the Beijing Internet Court considered originality insufficient for qualification as a work, whereas the Shenzhen Tencent case established that AI-generated works could indeed be recognized as such under Chinese intellectual property law.[68]

The divergent outcomes of the two cases serve as a promising incentive for AI pioneers to engage with the Chinese technology sector, contributing to the development of precise, ethical, and equitable legislation. This endeavour necessitates the creation of an innovation-friendly environment, where technology providers can innovate without excessive legal constraints while maintaining accountability for compliance with evolving regulations. Achieving this balance hinges on a proactive collaboration between the scientific and legal communities, facilitating transparent and mutually beneficial joint initiatives. By sharing the risks associated with AI advancements, both entities collectively assume responsibility for the outcomes and societal implications of their discoveries, fostering a more accountable and ethically sound AI landscape.

KEY TAKEAWAYS FROM CHINA

China's approach prioritizes centralized government authority in shaping legislative mandates. This approach ensures a structured and cohesive framework for AI regulation across the nation. If businesses in China adhere to the core guidelines outlined in the aforementioned national laws, they should experience minimal difficulty adapting to changes in AI legislation due to the coherence in legal principles nationwide. Nonetheless, businesses operating within China's advanced AI ecosystem must carefully assess their products for compliance with these rigorous requirements and prioritize the establishment of flexible procedural commercial frameworks that prioritize legal adaptability over profit, aligning with China's evolving and comprehensive AI regulatory landscape.

China also grapples with the rapid integration of AI and digitalization across society and the economy, and thus the emergence of stringent regulations becomes paramount. These regulations, propelled by concerns over privacy, personal data protection, and data security, have sparked legal responses and landmark cases, shaping the nation's AI regulatory landscape. China's legal framework encompasses a range of statutes, from the Personal Information Protection Law (PIPL) to the Data Security Law and Cybersecurity Law, collectively defining rules for data handling and privacy protection.

The analysis of the PIPL in comparison to the European Union's GDPR reveals significant parallels in data protection, underscoring the global significance of safeguarding data privacy. Furthermore, China's proactive stance is exemplified by its Development Plan for the Next Generation AI, outlining ambitious goals for AI legislation and governance by 2030, and the ongoing establishment of AI pilot zones to nurture AI industry growth.

However, two landmark cases, the Baidu and Tencent Dreamwriter cases, demonstrate a human-centric perspective, denying copyright interests to AI machines, while emphasizing the paramount importance of originality in determining copyright eligibility. Despite this, China's regulatory approach, as evidenced by its meticulous drafting of AI-specific regulations like the "Measures for the Management of Generative Artificial Intelligence Services," aims to foster ethical AI use and address societal challenges.

The multifaceted dimensions of China's AI regulation, its focus on accountability, transparency, and ethical AI usage, and the collaborative synergy between national and

municipal laws highlight the nation's commitment to governing AI comprehensively. As China fortifies its regulatory framework, businesses operating within its borders must navigate these complexities, ensuring compliance while adapting to evolving regulatory landscapes in the dynamic AI industry and most importantly fostering a collaborative relationship whilst collectively assuming the risk. This approach can prove promising in an era where cutting-edge technologies are developed at high velocities. The overlap and inherent cross-disciplinary nature of these frontier advancements makes it a better time than ever to have the legal and scientific communities work in tandem.

CONCLUSION

By comparing two approaches of AI regulation jurisdictions with a vast ideological gap, it is possible to attempt at identifying a spectrum for how nations will implement AI legislation. On the one hand, we have the EU with a comprehensive Act aiming at harmonising economic objectives while maintaining a firm regulatory grip over commercial activities relating to AI systems. This objective is underscored when exploring the emphasis and disclosure burden for High-Risk AI systems, a categorization likely to encompass a large number of solution providers. It will therefore be paramount for the EU to take advantage of the slow application of the AI Act, to probe how likely international organizations are to invest in the jurisdiction, as well as the likeliness of adoption by member states given the current version of the law.

On the other hand, China has clearly prioritized innovation when it comes to regulating AI nationally. By allowing various municipalities to have favourable legislative instruments that allow to boost efficacy in their areas of specialization, organizations will have the ability to navigate regulatory hurdles by applying strategic deployment of solutions within advantageous jurisdictions. Furthermore, joint ventures can be created when an organization is unable to overcome a regulatory mandate within their jurisdiction, thereby outsourcing AI development towards a favourable municipality for the task at hand. Although this flexibility may be attractive to AI system providers, it is important to understand that the Chinese government has full control over these laws and will not hesitate to halt innovation if it poses a risk to national security.

Consequently, it is evident that AI regulation is currently at a very early stage. However, the importance of moderation has been acknowledged by most states. Setting the standard for moderation by implementing revolutionary legislative instruments as the EU has undertaken,

will first benefit national security thus creating a sustainable environment for economic growth and social prosperity through the prioritization of safety over innovation. Protecting the people by policing the actions of organizations in emerging technologies will prevent market abuse, reduce misinformation, and discourage over-reliance on AI systems which can decrease human productivity.

Finally, the race towards AI hegemony has created a challenging environment for regulators to operate in, especially with nations like the US and China who blatantly prioritize economic prosperity over regulation. Therefore, it would not be surprising to see jurisdictions lagging in AI development sacrifice legal adequacy to promote innovation and become more attractive to foreign investors. Organizations will have to survey the global regulatory landscape and make strategic decisions on where to conduct their AI operations and tailor the products in alignment with the priorities of their jurisdictions to allow for effective lobbying. At the same time, nations will have to carefully assess the impact of these novel systems on their population. A prudent approach would entail taking a human-centric approach, which requires a strong focus on privacy programs, raising AI awareness in societies to equip individuals with necessary knowledge for safe utilization of these tools, and strict rules for AI providers to minimize opacity in their systems

---

[*] Sid Ali Boutellis has an LLM in Corporate Law from BPP University and is a candidate for SQE 2 in the UK. He has extensive experience in legal technology and is an advocate for AI regulation and data privacy. Credit to Dr. Ryan Cushley-Spendiff for remarkable editorial comments.

[1] Russell S and Norvig P, *Artificial Intelligence: A Modern Approach* (3rd edn, Pearson Education Limited 2016) 2

[2] Nabi J, *Machine Learning Basics Every Beginner Should Know*, (*BuiltIn* 17 November 2023) < https://builtin.com/machine-learning/machine-learning-basics > accessed 30 September 2024

[3] Brown S, *Machine Learning Explained,* (*MIT Management Sloan School* 21 April 2021) < https://mitsloan.mit.edu/ideas-made-to-matter/machine-learning-explained > accessed 30 September 2024

[4] Gillani N and Others, *Unpacking the "Black Box" of AI in Education*, (2022). Educational Technology and Society 26 (1) accessed July 2023

[5] Adam Morris, *What Is AI Without Machine Learning? (*4 August 2023) < https://futureforge.ai/what-is-ai-without-machine-learning/ > accessed 30 September 2024

[6] Zhang L and Others, 'Tropical Geometry of Deep Neural Networks' (International Conference on Machine Learning, Stockholm, 2018) < https://proceedings.mlr.press/v80/zhang18i.html > accessed 30 September 2024.

[7] Gillani N and Others, *Unpacking the "Black Box" of AI in Education*, (2022). Educational Technology and Society 26 (1) accessed July 2023

[8] ibid

[9] Simonyan K and Others, 'Deep Inside Convolutional Networks: Visualising Image Classification Models and Saliency Maps' (2014) arXiv.org e print archive < https://arxiv.org/pdf/1312.6034 > accessed 30 September 2024

[10] Aytekin C, 'Neural Networks are Decision Trees', (2022) arXiv.org e print archive < https://arxiv.org/pdf/2210.05189 > accessed 30 September 2024

[11] Gutbezahl J, 'Five Types of Statistical Bias to Avoid in your Analyses' (Harvard Business School 13 June 2017) < https://online.hbs.edu/blog/post/types-of-statistical-bias >Accessed July 2023
[12] Taylor R, 'AI Barometer Independent Report' (2020), Centre for Data Ethics and Innovation <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/894170/CDEI_AI_Barometer.pdf> accessed 29 September 2024
[13] Lai, Brian and Mamzer (n 18) 4.
[14] Jones C and Others, *Artificial Intelligence and Clinical Decision Support: Clinicians' Perspectives on Trust, Trustworthiness, and Liability,* Medical Law Review 31 (4) accessed 29 September 2024.
[15] Ibid
[16] Welford B, 'What is GDPR' (GDPR EU n.d.) < https://gdpr.eu/what-is-gdpr > accessed 23 July 2023
[17] Artificial Intelligence Regulation (EU) 2021/0106 (COD) of 21 April 2021 on Laying Down Harmonized Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts COM/2021/206
[18] General Data Protection Regulation (EU) 2016/679 of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC OJ L 119
[19] Zannoni L and Propato M, 'AI and GDPR: A Tight Affair' (Dentons, 20 April 2022) < https://www.dentons.com/en/insights/articles/2022/april/20/ai-and-gdpr-a-tight-affair > accessed 23 July 2023
[20] Blair T, 'Appropriate Safeguards in the GDPR: The EDATA Guide to GDPR' (Morgan Lewis 14 February 2019) < https://www.morganlewis.com/pubs/2019/02/appropriate-safeguards-in-the-gdpr > accessed 28 July 2023

[21] Scientific Foresight Unit, The Impact of GDPR on Artificial Intelligence, (European Parliamentary Research Service June 2020) < https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf > accessed 1 July 2023
[22] ibid
[23] Artificial Intelligence Regulation (EU) 2021/0106 (COD) of 21 April 2021 on laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts COM/2021/206
[24] Council of the European Union, 'Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts (Council of the European Union 25 November 2022) < https://data.consilium.europa.eu/doc/document/ST-14954-2022-INIT/en/pdf > Accessed 6 July 2023
[25] European Parliament P9 TA (2023)0236, Amendments adopted by the European Parliament on 14 June 2023 on the Proposal for a Regulation of the European Parliament and of the Council on Laying Down Harmonized Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts (COM (2021)0206 – C9-0146/2021 – 2021/0106(COD)
[26] European Parliament, 'EU AI Act: First Regulation on Artificial Intelligence' (European Parliament 08 June 2023) < EU AI Act: first regulation on artificial intelligence | Topics | European Parliament (europa.eu) > accessed 29 September 2024
[27] Future of Life Institute, 'EU Artificial Intelligence Act' (Future of Life Institute 13 June 20224) < The Act Texts | EU Artificial Intelligence Act > accessed 29 September 2024
[28] Directorate-General for Communication European Commission, 'AI Act Enters into Force' (Directorate-General for Communication European Commission 1 August 2024) < AI Act enters into force - European Commission (europa.eu) > accessed 29 September 2024
[29] European Parliament and Council of the European Parliament, Official Journal of the European Union, Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence and Amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance) PE/24/2024/REV/1
[30] Mauritz Kop, *EU Artificial Intelligence Act: The European Approach to AI*, Stanford Law School (2021) Stanford - Vienna Transatlantic Technology Law Forum, Transatlantic Antitrust and IPR Developments, Stanford University, 2/2021 accessed 23 July 2023
[31] ibid
[32] ibid

[33] Okrent A and Burke A, 'Participation of Demographic Groups in STEM' (National Science Foundation 31 August 2021) < https://ncses.nsf.gov/pubs/nsb20212/participation-of-demographic-groups-in-stem > Accessed 15 August 2023.
[34] National Institute of Standards and Technology, 'There's More to AI Bias Than Biased Data, NIST Report Highlights' (NIST 16 March 2022) < https://www.nist.gov/news-events/news/2022/03/theres-more-ai-bias-biased-data-nist-report-highlights> accessed 15 August 2023
[35] Maher K, 'Environmental Intelligence: Applications of AI to Climate Change, Sustainability, and Environmental Health', (Human-Centred Artificial Intelligence at Stanford University 16 July 2020) < https://hai.stanford.edu/news/environmental-intelligence-applications-ai-climate-change-sustainability-and-environmental > accessed 11 July 2023.
[36] Sutrop M, *Should We Trust Artificial Intelligence*. (2019). TRAMES Journal of the Humanities and Social Sciences, 23 (4) < https://www.researchgate.net/publication/337458067_Should_we_trust_artificial_intelligenc > accessed 6 July 2023
[37] Bryson, J, 'No one Should Trust Artificial Intelligence' (United Nations University 14 November 2018) <http://ourworld.unu.edu/en/no-one-should-trust-artificial-intelligence> accessed on 6 July 2023
[38] European Parliament and Council of the European Parliament, Official Journal of the European Union, Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence and Amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance) PE/24/2024/REV/1
[39] Wood T and Wihl L, 'Artificial Intelligence: An updated approach to EU liability legislation' (Deloitte 5 April 2023) < https://www2.deloitte.com/uk/en/blog/auditandassurance/2023/ai-updated-eu-liability-legislation.html > accessed 23 July 2023.
[40] Carabantes, M, *Black-box Artificial Intelligence: An Epistemological and Critical Analysis*. (2020). AI & Society 35
[41] European Commission, DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on Adapting Non-Contractual Civil Liability Rules to Artificial Intelligence (AI Liability Directive) (Text with EEA Relevance) COM 2022 496 FINAL
[42] ibid
[43] ibid
[44] European Commission, Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on Liability for Defective Products) (Text with EEA Relevance) COM 2022 496 FINAL COM (2022) 495 FINAL
[45] ibid
[46] ibid
[47] Wangwei L and Others, *Artificial intelligence in a digital age in China*. (2022). Company Lawyer 43(3)
[48] Webster G and Others, Full Translation: China's 'New Generation Artificial Intelligence Development Plan' (DigiChina 01 August 2017) < https://digichina.stanford.edu/work/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/> accessed 05 March 2025
[49] DigiChina, 'Translation: Data Security Law of the People's Republic of China (Effective Sept. 1, 2021)' (DigiChina Stanford University 29 June 2021) < https://digichina.stanford.edu/work/translation-data-security-law-of-the-peoples-republic-of-china/ > accessed 08 July 2023
[50] Creemers R and Webster G, Personal Information Protection Law of the People's Republic of China (Effective Nov. 1, 2021) (DigiChina Stanford University < https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/ > accessed 8 July 2023
[51] Brown M and Others, Dawning of a New Era: China's Personal Information Protection Law (Mondaq 03 September 2021) <https://www.mondaq.com/china/data-protection/1108072/dawning-of-a-new-era-chinas-personal-information-protection-law>
accessed 28 August 2023
[52] ibid
[53] ibid
[54] Band J, 'Israel Ministry of Justice Issues Opinion Supporting the Use of Copyrighted Works for Machine Learning' (Disruptive Competition Project 19 January 2023) < https://www.project-disco.org/intellectual-

property/011823-israel-ministry-of-justice-issues-opinion-supporting-the-use-of-copyrighted-works-for-machine-learning/> Accessed 28 August 2023.

[55] ibid

[56] Government of China, 'Notice of the Ministry of Science and Technology on Issuing the "Guidelines for the Construction of National New Generation Artificial Intelligence Innovation and Development Pilot Zones" (Government of China 06 September 2019) <http://www.gov.cn/xinwen/2019-09/06/content_5427767.htm> Accessed 1 September 2023

[57] Centre for Security and Emerging Technology, 'China Creates National New Generation Artificial Intelligence Innovation and Development Pilot Zones' (Center for Security and Emerging Technology (CSET) 11 March 2020 < https://cset.georgetown.edu/publication/china-creates-national-new-generation-artificial-intelligence-innovation-and-development-pilot-zones/ > Accessed 1 September 2023

[58] Huang S and Others, 'Measures for the Management of Generative Artificial Intelligence Services (Draft for Comment) April 2023' (DigiChina Stanford University 12 April 2023), < https://digichina.stanford.edu/work/translation-measures-for-the-management-of-generative-artificial-intelligence-services-draft-for-comment-april-2023/ > accessed 8 July 2023.

[59] Schildkraut P and Zhang H, 'What To Know About China's New AI Regulations' (19 April 2023) < https://www.arnoldporter.com/-/media/files/perspectives/publications/2023/04/what-to-know-about-chinas-new-ai-regulations.pdf?rev=d872d730384040619c1301e098cd90ee > accessed 8 July 2023

[60] Centre for Security and Emerging Technology, 'Regulations for the Promotion of the Development of the Artificial Intelligence Industry in Shanghai Municipality The Standing Committee of the 15th Shanghai Municipal People's Congress' (Centre for Security and Emerging Technology (CSET)15 December 2022) < https://cset.georgetown.edu/publication/regulations-for-the-promotion-of-the-development-of-the-artificial-intelligence-industry-in-shanghai-municipality/ > accessed 8 July 2023.

[61] Centre for Security and Emerging Technology, Regulations for the Promotion of the Development of the Artificial Intelligence Industry in Shenzhen Special Economic Zone (Centre for Security and Emerging Technology (CSET)15 December 2022) < https://cset.georgetown.edu/publication/regulations-for-the-promotion-of-the-artificial-intelligence-industry-in-shenzhen-special-economic-zone/ > accessed 8 July 2023.

[62] ibid

[63] ibid

[64] Beijing Film Law Firm v Baidu Netcom Technology Co Ltd [2018] Beijing Internet Court, Min Chu No.239

[65] Shenzhen Tencent Computer System Co Ltd v Shanghai Yingxun Technology Co [2019] Shenzhen Nanshan District Court, 0305 Minchu No.14010

[66] Kenneth-Southworth E and Yahong L, *AI's Future Impact on Copyright for AI-Generated Works: Insights from Chinese Case Law.* (2022). European Intellectual Property Review 44 (7)

[67] ibid

[68] Wangwei L, *Regulating Artificial Intelligence-Generated Content Services in China*. (2023). Company Lawyer 44(10)