

WestminsterResearch

<http://www.westminster.ac.uk/westminsterresearch>

Can Artificial Intelligence, RegTech and CharityTech provide Effective Solutions for Anti-money Laundering and Counter-terror Financing Initiatives in Charitable Fundraising.

Singh, C. and Lin, W.

This article is © Emerald and permission has been granted for this version to appear here: <http://westminsterresearch.westminster.ac.uk/>

Emerald does not grant permission for this article to be further copied/distributed or hosted elsewhere without the express permission from Emerald Group Publishing Limited.

The final, published version in Journal of Money Laundering Control, DOI: 10.1108/JMLC-09-2020-0100, 2020 is available at:

<https://doi.org/10.1108/JMLC-09-2020-0100>

The WestminsterResearch online digital archive at the University of Westminster aims to make the research output of the University available to a wider audience. Copyright and Moral Rights remain with the authors and/or copyright owners.

Can Artificial Intelligence, RegTech and CharityTech provide Effective Solutions for Anti-money Laundering and Counter-terror Financing Initiatives in Charitable Fundraising.

Singh, C.* , Lin. W.* and Ye, Z.*

Key Terms: Artificial Intelligence, RegTech, Anti-money Laundering, CharityTech, Counter-terror Finance, English Law.

Abstract

Purpose: Artificial intelligence has had a major impact on organisations from Banking through to Law Firms. The rate at which technology has developed in terms of tasks that are complex, technical and time consuming has been astounding. The purpose of this article is to explore the solutions that AI, RegTech and CharityTech provide to charities in navigating the vast amount of anti-money laundering and counter-terror finance legislation in the United Kingdom; so that they comply with the requirements and mitigate the potential risk they face but also develop a more coherent and streamlined set of actions.

Design/methodology/approach: The subject is approached through the analysis of data, literature and, domestic and international regulation. The first part of the article explores the current obligations and risks charities face, these are then, in the second part, set against the examination of potential technological solutions as at August 2020.

Findings: It is suggested that charities underestimate the importance of the nature and size of the threat posed to them, this is significant, as demonstrated, given the growing size and impact of the sector. Technological solutions are suggested to combat the issues charities face.

Originality: The work is original because it is the first to create the notion of CharityTech, and to specifically explore what technological advances can assist charities in meeting the regulatory compliance challenge.

Introduction

Artificial intelligence (AI) is changing the face of fundraising. The ability of AI to automate the tasks often considered as ‘tedious’ generates immense benefits for instance creating time for those seeking to raise funds to do the necessary strategizing and donor networking. AI, data analytics and machine learning (ML) may sound like commonplace buzzwords, but their potential is being built into organisation technology systems as innovative solutions to the issues relating to manpower or human resource, compliance and the management of risk. In this article we explore how AI, we have termed this CharityTech, can help alleviate a notable problem facing charities where fundraising is concerned; how to prevent their systems being used to launder money and finance terror. In so doing we investigate whether AI is a trustworthy component in the future of fundraising for the not-for-profit charity sector.

* C.Singh1@westminster.ac.uk . Dr. Charanjit Singh, Principal Lecturer in Law and Director of Learning, Teaching and Quality Assurance at the University of Westminster, a Barrister and Certified Civil and Commercial Mediator.

* Dr. Wangwei Lin is a Senior Lecturer at Coventry University Law School.

* Dr. Zhen Ye, Barrister, 3 PB Barristers.

1. Charities in the United Kingdom

Before considering the issues facing charities in terms of financial crime, both practically and theoretically, defining the organisations that are the subject of this research.

Charities', in England and Wales, are regulated organisations formed for particular charitable purposes. In law they are purpose trusts[1] without named beneficiaries. They fall into the voluntary sector but are distinguishable; the sector includes many other non-profit and non-charitable organisations. Often the charitable sector will be referred to as the 'third sector' alongside the 'public' and 'private' sectors. Sections 1 – 3 of the United Kingdom's Charities Act 2011 set out the legal definition of a charity, of charitable purpose and the description of that purpose. Save in short, the latter is to prevention or relief of poverty or the advancement of education or religion etcetera[2].

Charities may choose to set themselves up as companies[3] limited by guarantee with trustees as board members. Shell charities pose specific regulatory problems. A shell corporation[4] or company is set up in compliance with the relevant legislation and has financial assets but conducts little or no business activity. The purpose of this organisation is to act as a conduit through which financial transactions can be undertaken anonymously. Whilst they can be utilised for legitimate purposes i.e. asset storage for start-ups, they are often used for illegal purposes such as money laundering. Shell charities often fall into the latter category[5] and therefore pose a major financial crime risk. Regardless of the form they choose the principles that apply to 'charities' must be adhered to. It is salient to note that, whilst beyond the scope of this article, the rules of equity, various fiduciary duties and the duty of prudence, care and skill as set out in the Trustees Act 2000[6], all seek to regulate the actions of the decision makers within a charitable operation. The Charity Commission seeks to promote transparency in the financial affairs of third sector organisations with the main aim of sustaining and possibly increasing charitable giving. Maintaining 'donor' trust and confidence is important in this endeavour, something that is discussed in relation to AI later in this article. There are obvious financial i.e. tax benefits[7] to charitable status, this is a matter beyond the scope of this article but may present problems relating to fraud in its own regard for the exchequer.

In 2018, there were over 212,063 charities registered in the United Kingdom, 19,731 operating overseas. This poses a significant compliance challenge both for the authorities and the charities[8] as discussed later in the paper. It is salient to begin the discussion with the forms of abuse that charities face.

2. Charities and their Fundraising Aims

There is no human endeavour that is oft-presented more worthy of praise than not-for-profit fundraising. The traditional methods used to generate funds[9] namely; grants, networking and donor dinners, direct giving from corporate foundations, meetings in coffee shops etcetera need to be supplemented to fund what are often referred to in the charity sector as 'change-the-world initiatives'. AI provides an answer to achieving low human resource costs whilst maintaining high-levels of relationship-building and outreach as discussed later in the paper.

AI, of which ML is a constituent technology, allows a machine to act, comprehend, learn and sense just like an individual would. It is transformative; the relationship between people and machines is changing at a phenomenal rate, AI harnesses human ingenuity but does so with

alarming precision and speed. Recent experiments show that AI outperforms humans, and some of the best lawyers, in the completion of various legal functions[10].

Charities, like companies, also have large compliance and legal departments sometimes fragmented and potential liabilities, AI has benefitted the legal function in terms of the quality of information received by compliance officers and lawyers, and the speed[11] at which it can be reviewed by them which can lead to mitigation of regulatory risk and massive costs savings. One of the issues that the technology is grappling with is bias, it still needs to be ‘taught’ through data entry and confirmation by human subjects and that introduces potential pitfalls; including questions relating to the competency of the ‘teachers’, unconscious or subjective bias i.e. racial, gender or ideological biases, the production of biased data without due regard and assessment of its origins, a lack of critical thinking and trust[12] in decision-making. This problem persists throughout automation via AI but it is arguable that the benefits outweigh these issues because they can be rectified. IBM suggests that bias in AI occurs in the data or algorithmic models that are used[13]. AI also poses a significant risk to the compliance and lawyering functions as well as ethical issues but the automated settlement of disputes or ‘digital dispute resolution’ will benefit charitable organisations in terms of legal risk mitigation and notable costs savings[14].

In terms of fundraising there are a number of benefits. The many discussions on data analytics[15] (DA) will not be repeated in this article, the thrust of DA often involves using technology as a disruptor by changing the very foundation of how information works to promote a denser and richer higher-level collaboration amongst stakeholders. Benefits[16] include better targeted campaigns, creation of innovative and tailored products and for the purposes of this article to manage legal and regulatory risk[17].

3. Legal Problems with Charitable Fund Raising

Charitable spending in England and Wales totalled around £80Bn in 2019[18], this could rise to £146Bn by 2030[19]. Cybercrime, anti-money laundering, counter-terror finance and fraud are all matters that affect charities (GCHQ, 2020)[20]. The rise in the use of technology has resulted in an increase in ‘faceless’ crimes carried out by organised crime groups (Reichel, 2019)[21]. In addition, there has been a rise in relation to the number of fraudulent transactions too. Across the world financial crime has increased exponentially, Price Waterhouse Cooper’s Global Economic Crime and Fraud Survey (2020) revealed losses in the firms they work with across 99 territories to the value of \$42Bn[22]. The Financial Conduct Authority (FCA), the regulator of financial firms in the United Kingdom, suggests that in 2019, the serious and organised crime that money laundering facilitates costs the United Kingdom £37Bn every year, and the annual cost of fraud is estimated to be around £190Bn every year[23].

The FCA published a financial crime statistical analysis[24]. In 2018, there were 923,000 suspicious activity reports made by automated systems and employees to the Money Laundering Reporting Officers’ (MLRO) within those regulated financial firms within the United Kingdom, and after investigation 363,000 of these cases were reported to the National Crime Agency for further action, and it is salient to note that 2100 of these were terrorism-related[25] suspicious activity reports. The human resource cost to employ ‘checkers to check those checking’ is great, reductions in relation to which, that AI brings, is clearly advantageous.

The United Kingdom’s Serious and Organised Crime Agency (SOCA) identified various instances in which charities have been the victims of scams. In terms of fraud, charities, are

susceptible to fictional or fake payments, donations by mystery donors and loans as a means to launder money all to the detriment of the charity. What follows is a brief discussion of each of these.

3.1. The Fictional or Fake Payment

This is a common method of diverting funds to criminal organisations to launder money and fund organised crime and terror related activities. The fraudster will make a donation to the charity on the basis that part of the donation is made by it to a fictional charitable organisation in another country. The donation will be made using stolen details i.e. credit cards or other forms of payment, once the sum is received by the charity it then sends the conditional donation onwards. The fraud is uncovered at a financial institutional level and the total sum is recalled for which the charity is liable. By then the money has been laundered and the charity has become the victim of financial crime.

3.2. Mystery Donors

The second instance involves the disposal of the proceeds of crime to prevent detection and prosecution. Often, donors wish to remain anonymous for a variety of reasons. However, donations whether cash or otherwise, often through a third person, where the identity of the donor is withheld are used to dispose the proceeds of crime.

3.3. Loans

This is similar to the fictional or fake payment, here a donation is made with restrictions attached to it for example; it must be used for a specific project or with a particular company or organisation. This is a mechanism used to launder money by placing the proceeds of criminality into the financial system via the charity. The latter becomes the 'vehicle' through which the funds are then transferred overseas for instance a project paid for or the requisite partnership undertaken, and their origin is therefore disguised i.e. they have been layered. These monies are then often used in further organised crime or re-integrated through the purchase of assets.

Any loans where the charity is allowed to keep the monies for a set period of time and the interest accrued or earned, after which the principal sum must be returned indicates that this is a high-risk transaction. Also, loans made in one currency i.e. dollars (\$), with unusual conditions attached and then the loan must then be returned in a different currency for example pound sterling (£).

3.4. Tax Avoidance or Evasion

A donor may seek to benefit from tax relief on their donation but at the same time gain a private benefit for example they may insist that the donation be used to purchase services on beneficial terms from a company with which they are associated.

In trying to protect the charity trustees would try to identify suspicious activity for example large amounts of money, requirements or conditions precedent, complex banking and transfer methods, or loans disguised as donations. This when undertaken manually, as is the current practice across the charity sector, is a complex and time consuming endeavour which can be

very costly but is also subject to common human error which can lead to breaches of legal requirements. Technology can resolve this issue, the benefits of automation in relation to this are discussed later.

4. Economic and Financial Crime

The Organisation for Economic Co-operation and Development (OECD) outlines that economic and financial crime poses a major obstacle to development[26] because valuable resources are lost through criminal activity and this is particularly acute for fragile countries who are often the beneficiaries of charitable funds. These funds have a ‘spoiler’ effect, in that it money that should be used to rebuild public services i.e. education, health, justice and security are diverted.

4.1. Governance and the Compliance Toolkit

Charities owe particular legal duties as set out in the Charities Act 1992, Charitable Institutions (Fund-Raising) Regulations 1994 and the Charities Act 2006 and now the Charities Act 2011. Before discussing the legal framework in which anti-money laundering and counter-terror finance exists within the United Kingdom (*ibid*), it is salient to outline some areas of the basic regulatory compliance scheme.

The simple way in which charities can prevent themselves becoming the victims of crime and financial abuse is to have proper governance and management procedures, and effective financial controls in place. For instance the adoption of ‘Know Your Customer’ (KYC) and ‘Due Diligence’ (DD) procedures on every transaction i.e. money coming into and going out from the charity and those that work with it. These are grounded in the legal duties of the trustees, designed to protect the assets of the charity and are referred to as the ‘Know Your’ principles[27]. Charities must have and carry out DD to mitigate financial crime, financial institutions require this of them. Thus, charities need to have risk-based processes know about their affiliated organisations, beneficiaries, donors, employees, partners, suppliers and volunteers. The risk-based approach means a greater level of due diligence is required, this should form part of a financial crime policy that is agreed by Charity’s the Trustees. Many organisations struggle with regulatory compliance because of the issues of using paper-based systems which are, amongst others, human fatigue, forgetfulness, sloppiness and time pressure.

The problems of charities being misused are more acute where they are operating in countries that have been sanctioned or those that are higher risk or where they are dealing with ‘Politically Exposed Persons’ (PEPs). In terms of the latter corruption is a particular concern. They must comply with the sanctions and any other export control laws too. Terrorists often exploit these situations[28].

The problem is further exaggerated by increasing levels of regulation which leads to the requirement for continuous updating and symptomatically rises in compliance costs i.e. fines, business disruption and productivity loss and budgets[29].

The Charities Commission’s Compliance Toolkit[30] helps charities verify the end use of charitable funds, it states that ‘... ensuring proper internal and financial controls and risk management procedures are in place and implemented is vital’[31] but it does suggest an adequate set of solutions, technological or otherwise in this regard. Therefore, whilst the online toolkit is a small step towards clarity it is not one that aids resolution of the problems. The

‘grey’ areas on application of the rules and reporting still exist[32]. It is not automation of the regulatory compliance function, and charities are not using basic AI in that regard[33]. The guide is not, at the most basic, even machine-executable principles that internal AI based compliance systems could utilise to automatically update systems and processes without human interference akin to that being promoted in financial services compliance reporting[34]. The toolkit falls prey to the same human-factors which are eradicated by automation and therefore charities are failing to take advantage of potential reductions to the costs of non-compliance.

5. Legal Duties Counter-terror Finance (CTF) and Anti-money Laundering (AML)

5.1. Terror Financing

The United Kingdom has an extensive regime for the prosecution of terror criminal offences, these are contained in the Terrorism Act 2000[35] (TA), in force as at 19.02.2001. At an International level there exists a lack of consensus and an obvious ideological struggle in seeking to define terrorism[36]. This means that the definition varies across jurisdictions, creating an obvious compliance issue for charitable organisations. The TA 2000 defines terrorism as ‘the use of a threat or action that is designed to influence a government or international governmental organisation or to intimidate the public or a section of the public; made for the purpose of advancing a political, religious, racial or ideological cause and which involves or causes serious violence against person(s), serious damage to property, a threat to life, a serious risk to the health and safety of the general public or serious interference with or a disruption to an electronic system’[37]. It is also salient to note that the European Union’s Council Framework Decision on combatting terrorism 2002/475/JHA introduces a specific and common definition of terrorism.

Terrorists need to access money and property (assets) to organise as a group, buy weapons, to travel, accommodate and train so that they may co-ordinate, plan and execute their attacks. They may engage with legitimate organisations to generate income, the differences in geographical location may make detection impossible. Terror attacks are often carried out by small groups often using small amounts of money. Although, the size of the money seems minimal in risk terms they present a great challenge for charitable organisations in terms of terror finance and money laundering (the latter is discussed later). Thus, cutting-off the supply of money and assets to them is probably the most effective way of fighting terrorism and preventing future attacks. The outcome is to disrupt their material support, reduce their purchasing power and their ‘transaction histories’ i.e. withdrawal, transfer of funds and digital purchases provide valuable evidence for investigating and prosecuting authorities. This raises two interrelated issues; the first is absolute regulatory compliance which will vary according to the jurisdiction within which the charity is operating a problem exaggerated by cross-jurisdictional operations; like any other organization, the charity[38] must also develop mechanisms to ensure that it is not being unwittingly used to finance terror. The second, this level of regulatory compliance is problematic for charities seeking to maximise operational cost efficiency.

The legislation creates a number of criminal offences relating to terrorism and one of the most relevant, for the purposes of this article, is fundraising, financing, encouraging and supporting terrorists. The legislation gives investigating agencies (police) powers and the TA 2000 allows the Home Secretary to ‘proscribe’ organisations. For charities, and the trustees, this is particularly relevant in terms of proscribed groups, the duty to report suspicions and terrorist

financing is concerned. The Terrorist Asset Freezing Act (etc.) 2010 an entity or person can be 'designated' where HM Treasury has reasonable grounds to suspect (for interim designation) or believe (for final designation) that (a) they are or have been involved in terrorist activity and (b) they are owned, controlled or acting on behalf of or at the direction of someone who does[39].

Sections 15 – 18 of the TA 2000 creates a number of offences some of the most relevant to charities include; raising funds or donating money to a proscribed organisation; receiving or providing money or property where it is intended or where there is reasonable cause to suspect that it may be used for the purposes of terrorism; facilitating money laundering and failing to report suspicions of terrorist finance offences to the police. The Terrorism Act 2008 amended the 2000 Act, it is now clear that the reporting requirements i.e. where there is belief or suspicion, apply to charities and their trustees.

The Terrorism Asset Freezing etc. Act 2010, amongst other things, makes it an offence to make funds, financial services or economic resources available for the benefit of a designated person. The Counter Terrorism and Security Act 2015 places the Prevent Duty[40] on a statutory footing; it applies to Higher Education Institutions and Colleges (Tertiary Education) in the U.K., these may be registered as charities and must ensure compliance.

Specifically, it is an offence for a charity to provide funds to proscribed individuals and/or organisations, to any organization it suspects as being a terrorist one. The salient point to note is that in relation to the latter it may not appear on any of the lists relating to proscribed organisations or individuals. In terms of the challenge, continuous manual physical inspection and audits are required something that AI do without the additional manpower with a higher level of accuracy (as discussed later).

This is relevant to both charities and anyone raising money for charities that are registered or charitable causes i.e. fundraisers, volunteers and the trustees themselves. If they have a 'reasonable cause to suspect' that the money they are raising may be used for terrorist activity they will have technically committed an offence contrary to the TA 2000 as amended. Interestingly, the offences can be committed by donors if they know or suspect that it will be used for terrorism.

The risk is not mitigated if the activity takes place overseas. Section 63 of the TA 2000 states that U.K. nationals and residents who commit an act(s) overseas which, if committed domestically, would amount to a terror finance act per ss.15 – 18 then they will have committed an offence and will be subject to relevant due process. Therefore, charities operating internationally must make sure their actors overseas stay within the requirements of U.K. law, another issue that AI can quite easily resolve – we will discuss the practicality later in this research.

The problems or abuse (financial) suffered by charities can take a number of different forms. The most common[41] are as follows;

- Establishment of a charity as a conduit through which monies can directly or indirectly fund terrorism;
- Public collections that are in the charity's name or for particular causes i.e. humanitarian crises and natural disasters, the funds are then used to finance terror activity without the charity's knowledge;

- The diversion of charitable funds when transferred into different currencies digital or via cash transfer and places, here the beneficiary never receives the money;
- The transportation of funds using a charity's name so as to avoid being questioned or challenged by the relevant authorities;
- Simple misuse of charitable donations, received for purpose A but expended on furthering terrorism; and
- Money laundering (discussed later).

Charities that operate in high-risk places i.e. Syria and Iraq, where the charity has a low annual income or those that are newly registered are particularly open to abuse[42]. Even though, the problem of charity involvement in terrorism being relatively small in relation to the cumulative size of this third sector does not detract from the compliance requirements in law, but also from the perspective that criminals will always seek weak links to exploit and such scandals undoubtedly damage the reputation, trust and confidence that the public place in charities and their work. It is salient to state that 'respect, trust and confidence', with all commercial enterprise[43] and where charities are concerned, has commercial value that must be properly protected. Charities must have proper risk-based policies and procedures, and systems to ensure they are not the victim of abuse, the automation of which has taken place in many industries already i.e. RegTech, FinTech and InsureTech[44].

In sum, charities must ensure that the obligations set out in U.K. anti-terrorism legislation are discharged effectively. That charity trustees not only comply with the law but are vigilant in making sure that the charity's assets i.e. property including premises, its staff, volunteers and other resources are not used for the promotion or support of terrorism as outlined.

5.2. Money Laundering

Money laundering is unlawful as set out in Part Seven of the Proceeds of Crime Act 2002 (POCA). In contrast to terror finance which concerns the illegitimate use of legitimate money, money laundering is the reverse. Here charities can be used as the mechanism through which illegitimate assets are converted into legal or legitimate ones. In this instance, criminal acts generate profit for the person or group, often organised criminals or drugs cartels, through the conversion of illegal gains into legitimate untraceable money. This is the process where the proceeds of crime are disguised so that they may then be enjoyed without bringing into jeopardy the source from which they came[45]. This is completed via a three-stage process; placement[46], layering and integration. What follows is an overview, a discussion beyond this is outside the scope of this article.

In stage one, the criminals place the profits of crime into the financial system i.e. a single or a number of banks. The money may come in the form of several small sums[47] to avoid easy detection, even by the most experienced of officers, so as to frustrate the possibility that a Suspicious Activity Report (SAR) per the legal requirements will be raised, something AI can easily achieve (discussed later).

In stage two, the ill-gotten gains are layered, transactions are made to distance the money from its original source, for example shell charities are legitimately created but with the primary purpose of receiving such assets in the form of donations. In stage three, the final of the stages; the money is integrated back into the 'white' economy[48] i.e. purchase of assets or making loans. The use of conditions in donations requiring the money be spent on a particular project or partner, the latter may be a complete fiction, are examples of this, as is the use of shell

charities that can enter into various financial transactions without revealing particular information whereby the origin of funds can be hidden.

The detection of this activity, patterns of behaviour that raise suspicion is difficult and can be labour intensive, therefore costly. Again, matters that AI can easily tackle, but that requires requisite financial investment that can pay dividend in the long term, where costs are concerned, but also in terms of regulatory compliance.

5.3. *International Regulation: Financial Action Taskforce (FATF) and the U.K. Charities Commission*

The Financial Action Task Force (FATF) is an intergovernmental global terror finance and money laundering watchdog that sets international standards aiming to prevent both these activities and mitigate the harm caused to society. Its 'recommendations' or standards, try to ensure a consistent global response to current and new risks, 200 nations have signed up to implementing them. Much of the domestic legislation, including EU Law, is based on these standards i.e. The Fifth Money Laundering Directive (EU) 2018/843 and Statutory Instrument (SI) 2019 No.1511 Financial Services, The Money Laundering and Terrorist Financing (Amendment) Regulations 2019. FATF suggests that the United Kingdom's counter-terror finance policy has three parts; deter via safeguards and supervision, detect through financial intelligence i.e. information garnered from money laundering controls so that the actors can be identified and targeted, and disruption by seizing assets and prosecution[49].

The Charity Commission in England and Wales[50], the regulator and supervisor of charities' in the United Kingdom, can investigate a charity for abuses and issues guidance on regulatory compliance etcetera. The Commission, like other regulators in the United Kingdom, tries to strike a balance between effective but not overburdensome regulation, innovation and efficiency. In so doing, it approaches its function to; raise awareness, oversee, supervise, co-operate and intervene where necessary[51]. Chapter 1 Module 8, of the Compliance Toolkit requires charity trustees to:

- Comply with the law;
- Act within the charity's interest, avoid it being exposed to undue risk and its assets are used only for its charitable purposes. In so doing, the trustees must:
 - o Take reasonable steps to ensure its premises, assets, employees (etc.) cannot be used for activities that may, or appear to, support or condone terrorism or terrorist activities;
 - o Put in place and implement effective procedures that prevent terror organisations taking advantage of the charity's assets, facilities, reputation or status;
 - o Take immediate action to disassociate the charity from activity outline in point 1 above;
 - o Take all reasonable steps to ensure that the activities of the charity are transparent and open, and cannot be misinterpreted;
 - o Safeguard the charity's assets;
 - o Ensure that proper control is exercised over financial affairs;
 - o Concerns about a charity's links with terrorism should be reported by any stakeholder i.e. beneficiary, employee or trustee[52].

5.4. Charities: Further TF and ML Problems

The range of risks charities face have already been highlighted, there are however a number of further abuses that require consideration too. Charities, unlike other company forms, are especially attractive to criminals because they are often perceived as being outside the regulatory gaze. This perception is challenged by the continued extension and application of law i.e. the criminalisation of acts or omissions, to charitable organizations; thus, charities should make more intelligent use of AI, the benefits of which they are not currently harnessing. FATF Recommendation 8, 'Combatting Abuse of Non-Profit Organisations', is particularly good example[53]. Thus, Charities are very much within the regulatory gaze domestically and internationally regardless of their size[54]; compliance with financial sanctions regimes is a good example of this. Adherence with the Charities Commission's Governance Code (2017)[55], which incidentally is neither law nor binding, is considered to be 'good governance' and adopts the 'comply or explain' position of the UK Corporate Governance Code[56].

5.5. CTF and AML Risks

There is a lack of universal criteria on the determination and assessment of the risk terror finance risk that is posed in particular countries or regions. There are however identified nations that pose significant risk to charities that must be mitigated, these are nations that may be subject to United Nations sanctions or embargoes[57]. The United Kingdom's Foreign and Commonwealth Office (FCO), Transparency International[58], FATF and the World Bank are credible sources from which it can be deciphered that particular countries have a lack of legislation on counter-terror finance and money laundering. There may be regions that are notorious terrorism hotspots, areas with criminality, corruption[59] and sparsely populated areas with poor infrastructure and of course those areas with internal strife (civil war or conflict, militia) or military warfare. Thus, charities operating abroad (internationally) must consider these matters when carrying out its risk assessments, specifically the circumstances relevant to the particular country or locality[60]. The factors that affect risk, for assessment purposes includes, the protection under the law, political environment, local law, culture, economic structure, concentration of illegality/criminality, levels of illicit trade/money, government controls, maturity and size of financial services infrastructure, market and institutions, reliability of the service sector etcetera.

5.6. Other Legislation

Given what has been discussed so far, charities must also navigate further financial crime and other legislation, the Companies Act 2006 has already been mentioned, particular reference also needs to be made the Bribery Act 2010. In addition, there continue to be advances where data protection is concerned which Charities, like others, must engage with. The European Commission's Whitepaper 'Artificial Intelligence - a European approach to excellence and trust' proposes a new regulatory framework for AI, not just to speed up its uptake, but also to tackle the human and ethical implications in its use i.e. opaque decision making and bias (Long and Agyekum, 2020). In July 2020, the UK's Information Commissioner Officer's (ICO) also published guidance on the best practices in data protection-compliant AI.

5.7. Financial Crime Policy (FCP)

Charities must have extensive financial crime policy that covers the legislation discussed, in addition to appropriate level operational risk assessments. These must set out the course of action that is required where a risk presents itself and the limits of risk in terms of appetite, standards and objectives; this should guide the operations. This (these), should be accompanied by procedures for implementation. To accompany this, stakeholders such as trustees, employees and volunteers need to be appropriately trained. The level and systematic alerts required will also vary so that risk is effectively mitigated. There also need to be measures in place for identification of suspicious activity, reporting and robust scrutiny and review so that lessons can be learnt. The FCP needs consistent and regular updating for example when legislation changes, organisations or individuals are designated, sanctions are lifted, or new ones imposed. Furthermore, criminality does not stand still, criminals find novel ways in which to circumvent detection and prevention, smurfing is a good example of this, therefore any FCP also needs to consistently develop – something that AI outperforms humans in relation to. Readers will begin to note the arduous task, in terms of regulatory compliance, that charities face, challenges that AI can easily help navigate.

6. CharityTech: Artificial Intelligence and Machine Learning

In this part of the research we focus on the use of technology to resolve the issues identified earlier.

Artificial intelligence (AI) refers to technology that enables a machine to simulate the behaviour of humans i.e. data, course intelligence, knowledge and understanding, it is therefore the ‘brains’ within, for instance, a robot. Therefore, AI systems are smart like humans and able to solve complex problems. In contrast, machine learning, which is a subset of AI, allows the machine to automatically learn from past data without the need of specific programming. RegTech, or what can be termed as CharityTech, is the use of information (data) and technology for purposes of ensuring, as far as can be possible, regulatory compliance and reporting, mitigating risk, training and developing staff, and harnessing cost reductions. It is salient to note that information is currently shared via memorandums of understanding between the various charity regulators, amongst others, Charity Commission, Information Commissioners Office and the Gambling Commission. Digital data can make this process far more effective and less costly.

The process is far more than just the digitization of manual compliance and reporting functions i.e. KYC requirements. The potential is to enable real-time changes and monitoring to take place and facilitate far more efficient and proportionate regulatory regimes that look to address existing and contemporaneous risks. Data, regulation and security (identity etcetera) can be relatively easily interwoven to achieve this.

7. Helping to Solve ‘the’ Problems: CharityTech and RegTech

The FCAs ‘Regulatory Sandbox’ circa 2015, has aided the revolution in the use technology can be used in novels ways to resolve complex and detailed regulatory compliance problems, as have similar schemes across the FinTech[61] spectrum.

An AI and ML digitalization, like that which has cut across many other industries and markets such as finance, law, banking and insurance, can bring serious cost saving, compliance and risk mitigation benefits for charities. Charities spending on costs is contentious where donors are concerned, in 2019 10 of the most popular charities in the UK spent over circa £225Mn on

operating costs[62]. The reductions that can be harnessed are salaries, office space, travel expense and some marketing costs, this list is not exhaustive. The first has obvious impact on donor confidence in the charity and revenue generation, given AI and ML can work 24/7 to provide service to internal users and donors etc.

From a compliance (CharityTech) perspective organisations can prevent themselves becoming the victims of financial abuse and criminality by having good management and governance procedures i.e. the Charity Commissions Governance Code, as well as proper financial controls. This will mean that timely audit, training, review and proper risk-based approach to Know Your Customer (KYC), Customer Due Diligence (CDD) and Know Your Principles (KYP) is undertaken to ascertain the source of funding and the identity of the beneficiary's. In terms of the latter the charity must understand that it is an offence to provide funds to organisations and individuals that are proscribed and therefore any 'system' must be subject to regular updating and be capable of sharing and identifying the same for risk mitigation purposes.

Specifically for charities that operate overseas, they must ensure that they comply with domestic (U.K.) regulation (including those set out in 3.1.2.) but also that of the jurisdiction in which they operate. Charities must ensure that they are not breaching sanctions regimes and embargoes. Furthermore, given the lack of universal criteria on how to assess the risk of terror finance by country and region, it is all the more important to have a series of models that can be used for the mitigation of this risk. The system in place will need to flag up 'hotspots', civil strife, terror attacks and other information that affects operations but also compliance. Therefore, it must be able to update in real-time by feeding in huge amounts of data and information from a multitude of sources if it is to be effective i.e. from the United Kingdom's Foreign and Commonwealth Office (FCO), Financial Conduct Authority, The Charity Commission, Transparency International, FATF and the World Bank. All of this requires time, money and creates the need for consistent updating of policies but also retraining for staff etc.

The policies, processes and people need to be able to facilitate suspicious transactions and patterns of behaviour being spotted from copious amounts and complex data, including smurfing as discussed earlier and that too in real-time before it is too late to take action i.e. the issuing a Suspicious Activity Report (SAR) and regulatory reporting; a very labour intensive and costly process. Breaches will not only result in loss but also a negative impact on reputation, and donor trust and confidence. Remedies, in law, against charities that fall foul of the law include breach of trust, removal of trustees and to direct how charity property is applied[63].

Charities are also at threat from cyber risks i.e. hacking etc. Therefore, other than the Companies Act 2006, the organisations must also secure its data from digital criminality[64].

All of these matters require an extensive and regularly up-to-date Financial Crime Policy something that charities struggle with. These are all matters that automation, digitalisation or RegTech (CharityTech), can assist with.

8. How Can Advances in AI, RegTech and CharityTech be a solution?

Charities must accept that they need to build their own networks to combat criminality through sharing information perhaps through privacy enhancing technologies (PETs) that could allow data sharing between charities, law enforcement agencies and regulators, and through nascent concepts such as homomorphic encryption[65].

The FCA's Regulatory Sandbox has seen various propositions into digital identity, that is securing information that is held by organisation. Whilst the technology centres on allowing businesses to check the identity of its customers digitally, machine learning avoids the need for a manual security check, the same can be implemented by charities if they adopt the 'open banking model' that allows the approved secure sharing of some information electronically via an application programming interface (API) perhaps with the financial institutions themselves.

The benefit is federated system of real-time updating, financial analysis i.e. donation receipts, beneficial ownership and tracking of grants, and identification and information sharing that combats financial crime. In addition, flags are raised where a 'high risk' donation or pattern is identified which allows the system to carry out further KYC or CDD.

Charities, like other organisations, face efficiency challenges in manual systems that seek compliance and risk mitigation etcetera. These include;

- Lack of up-to-date information;
- Human error;
- Continuous cost of stakeholder training and development;
- Poor quality data that needs to be cross-checked and corrected;
- Fragmentation of data affecting decision making;
- Increasing costs of manual KYC and CDD;
- False positives in risk analysis resulting in the misallocation of resource i.e. investigation of low risk activity or transactions. When calibration tools are added this only exaggerates the false-positive problem;
- Inconsistency in processes, standards and application violating regulatory compliance;
- Absence of centralised CDD or KYC database;
- Inconsistencies in suspicious activity reporting;
- Production of too many or too few reports or analyses;
- Duplication of processes;
- Fragmentation of systems that do not interact, resulting in employees having to (a) collect data and then (b) analysis the differences between the datasets manually which is prone to high error rates;
- Unreliable processes that cannot adequately assess risk from qualitative and quantitative metrics and geographies.

These are just to name a few, other than those already discussed. Technology can be used as an enabler but must have the necessary investment as a strategic approach; including:

- Automation of processes that are information centric to reduce manual data collection, entry and updating;
- Using e-KYC and e-CDD;
- Building and sharing KYC and CDD;
- Using web-based applications to audit, identify, track, trace, report, carry out link analysis (determine beneficial ownership) and interact with other stakeholders; and
- Using linguistics in data analysis.

Regulatory compliance has undergone a sea change; ethical culture, compliance and infrastructure – this is the core of anti-money laundering and counter terror finance initiatives but also are important in relation to organisational retraining, controls and governance.

9. Conclusion

Presently, charities are yet to harness the benefits of the technological revolution that is happening in other sectors. They have an opportunity to solve these problems by turning to AI and ML, or as it can be termed RegTech or CharityTech; rapid automation, advanced statistical modelling, voice analytics, real-time data aggregation platforms that use fuzzy logic and text analytics, and machine learning-based risk assessments. What is required is are further digital transformation initiatives. All of which have far better performance than the manual processes that are deployed. All of this has global benefits, given the size of the global charity sectors and the fact that perpetrators operate transnationally. This opportunity will help charities cut their operational costs and improve compliance but also donor trust and confidence; there must be a shift to looking forward towards a sustainable approach, growth in the charity sector means the problems will only grow. Technology and advanced analytics can help increase effectiveness and efficiency. Rather than expanding their people base, surgical automation and analytical tools can help charities comply, mitigate risk and fight the crime.

Endnotes

[1] A charitable purpose trust is a public trust set up for the purposes of providing a benefit to the public or a section thereof. They are regulated by the Charity Commission. The trust must be established for a purpose that is wholly and exclusively charitable as defined in law, any deviation will render it void. The outcome of any failure is dependent upon when it fails; if initially and the charitable intention is general the monies or property can be applied to similar purposes by application of the Cy-pres Doctrine. Where the failure is subsequent the doctrine has automatic application. For a detailed discussion see; P. S. Davies, G. Virgo, and E. H. Burn. *Equity and Trusts: Text, Cases and Materials*. (Oxford University Press, 2016 at Ch.5, pp.175 – 6).

[2] Section 3 provides a list of 13 descriptions that amount to charitable purposes including animal welfare and community development (etc.), therefore, the in-text reference is not exhaustive. For completeness you may wish to refer to *Commissioners for Special Purposes of Income Tax v Pemsel* [1891] AC 531, the Recreational Charities Act 1958 and the Charities Acts 1992, 1993 and 2006, as a background to whence the current form of the law came. Charities Act 2011, Chapter 25. HMSO: UK. Available at: <http://www.legislation.gov.uk/ukpga/2011/25>. [Accessed 13 April 2020]. See also: H. Picarda QC. *Law and Practice Relating to Charities*. (4th Ed., Bloomsbury Professional, 2010). Note the edition has been updated, the First Supplement to the 4th Ed. covers the 2011 statute, Part I at pp.3 – 45.

[3] Company Law Act 2006 will also apply to charities; compliance with a dual regulatory regime required. Sections 171 – 177 of the 2006 Act apply to directors of incorporated charitable companies. For those that are unincorporated there may be contractual liability in addition to liability for breach of the purpose trust. Under the Insolvency Act 1986 trustees may be personally liable for wrongful or fraudulent trading. It should be noted that s.191 of the Charities Act 2011 allows the Charity Commission to absolve the trustee from whole or partial liability where he or she has acted in a manner that was honest and reasonable.

[4] These organisations are normally set up in tax havens, they hide the identity of the owners, but this form allows them to engage in financial transactions, buy and sell property and own

copyrights as well as the collection of royalties. For a further discussion see; A. Ottavi. *Shell Corporations and Beneficial Owners. Current Criticalities and Future Developments from a Multilevel Perspective*. Bus. (2019) L.R. 40(3), 116-123. Also below: Barr, W. at note 28.

[5] Kingston, K. G. *Concealment of Illegally Obtained Assets in Nigeria: Revisiting the Role of the Churches in Money Laundering*. A.J.I.C.L. (2020) 28(1), 106-121. Whilst the focus of the article is Nigerian Churches, it demonstrates the common problems facing the excepted charity sector i.e. religious places of worship where the turnover is less than £100,000 per annum, such organisations must still comply with the law.

[6] See *above*, note 3.

[7] In the financial year 2018 – 2019 tax relief for charities in the United Kingdom totaled £3.79Bn, this was up from £3.62Bn in the financial year 2017 – 18. Individual tax relief for the same period totalled £1.53Bn. Gov.UK. (2020). HMRC Annual Statistics: UK Charities Tax Relief, Table 2. [ONLINE] Available at: <https://www.gov.uk/government/statistics/cost-of-tax-relief>. [Accessed 14 April 2020]. For a discussion on international approaches to regulation see; O. B. Breen. *Through the Looking Glass: European Perspectives on Non-Profit Vulnerability, Legitimacy and Regulation*. 2011 Vol. 36 No. 3 Brooklyn Journal of International Law at pp. 948-991; *UCD Working Papers in Law, Criminology & Socio-Legal Studies* Research Paper No. 47/2011. Available at SSRN: <https://ssrn.com/abstract=1932653>. [Accessed 14 April 2020].

[8] FATF. (2018). Anti-money laundering and counter-terrorist financing measures – United Kingdom. Fourth Round Mutual Evaluation Report, FATF, Paris, p.99. Available at: <http://www.fatf-gafi.org/publications/mutualevaluations/documents/mer-united-kingdom-2018.html>. [Accessed 12 April 2020].

[9] K. S. Sheldon. *Successful Corporate Fund Raising: Effective Strategies for Today's Non-profits*. Wiley Non-profit Law, Finance and Management Series. John Wiley & Sons 2000 at pp. 4 – 6.

[10] Sahota, N. and Ashley, M. (2019). Own the A.I. Revolution: Unlock Your Artificial Intelligence Strategy to Disrupt Your Competition. USA: McGraw-Hill Education. It is estimated that AI will have usurped many job functions in law (paralegal, researcher and compliance) by 2030. See: N. Sahot. *Will A.I. Put Lawyers Out Of Business?* Forbes 2020. [ONLINE]. Available at: <https://www.forbes.com/sites/cognitiveworld/2019/02/09/will-a-i-put-lawyers-out-of-business/#50e71e9e31f0>. [Accessed 31 March 2020].

[11] K. Leary. *The Verdict Is In: AI Outperforms Human Lawyers in Reviewing Legal Documents*. Futurism, 2020. [ONLINE]. Available at: <https://futurism.com/ai-contracts-lawyers-lawgeex>. [Accessed 01 April 2020].

[12] F. Ross. *Building Trust in Artificial Intelligence*. *Journal of International Affairs*. (2018) 72(1), pp.127-134. [Accessed 31 March 2020].

[13] R. K. E. Bellamy et al. *AI Fairness 360: An extensible toolkit for detecting and mitigating algorithmic bias*. IBM Journal of Research and Development, vol. 63, no. 4/5, pp. 4:1-4:15, 1 July-Sept. 2019. Also see the AI resource centre: IBM. *Mitigating Human Bias in AI*. 2020.

[ONLINE]. Available at: <https://www.research.ibm.com/5-in-5/ai-and-bias/>. [Accessed 31 March 2020]. See also: J. Wood, J. *This AI outperformed 20 corporate lawyers at legal work*. World Economic Forum 2020. [ONLINE]. Available at: <https://www.weforum.org/agenda/2018/11/this-ai-outperformed-20-corporate-lawyers-at-legal-work/>. [Accessed 01 April 2020].

[14] K. Beioley, *Robots and AI threaten to mediate disputes better than lawyers*. Financial Times 2019. [ONLINE]. Available at: <https://www.ft.com/content/187525d2-9e6e-11e9-9c06-a4640c9feebb>. [Accessed 01 April 2020]. See also: J. Hornle. *Dispute resolution: digital alternative*. June 16, 2014. Law Society Gazette.

[15] EMC Education Services. (Ed.). *Data Science and Big Data Analytics: Discovering, Analysing, Visualizing and Presenting Data*. John Wiley and Sons 2015.

[16] Other benefits include out-going correspondence that is written by AI i.e. ML tools, these can learn to mimic an author's writing style and respond to incoming communication. These tools can aid maximisation of efficiency in terms of travel itineraries and target those donors that are most likely make a gift or donation; AI fundraiser tools are able to sift through copious amounts of data in seconds, something that may take even the most senior employee's days or even weeks to do. AI technologies can also help target the funds where they are required most, therefore the adoption of these tools has become a question of 'when' rather than 'if'.

[17] M. Whalley and C. Guzelian. *The Legal Risk Management Handbook: An International Guide to Protect Your Business from Legal Loss*. Kogan Page 2016. Note: this book provides a good discussion of the management of legal risk and compliance, its management and relationship to issues of corporate governance. See also: D. Carlisle. *FinTech: The Next Frontier*. Money L.B. 2017, 249, 8-11 and T. Mallo. *Fine Words*. Money L.B. 2007, 141, 1-3. [Accessed 03 February 2020].

[18] Charities Commission for England and Wales. (2019). *Preventing Charity Cybercrime. Insights + Action*. Fraud Advisory Panel. [Online]. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/840997/Web_CC_Cyber.pdf. [Accessed 01 April 2020].

[19] Third Sector. (2013). *Global charitable giving could reach £146bn by 2030, says Charities Aid Foundation report*. [ONLINE] Available at: <https://www.thirdsector.co.uk/global-charitable-giving-reach-146bn-2030-says-charities-aid-foundation-report/fundraising/article/1172356>. [Accessed 12 April 2020]. There are no global statistics on charitable giving. The figures in the United Kingdom (above) and United States of America have demonstrated increases in donations. For the latter see: Non-profits. (2018). *Charitable Giving Statistics, Trends & Data: The Ultimate List of Charity Giving Statistics*. [ONLINE] Available at: <https://nonprofitssource.com/online-giving-statistics/>. [Accessed 12 April 2020].

[20] *Cyber Security Guide for Charities*. GCHQ: National Cyber Security Centre. UK: HMSO. [Accessed 15 April 2020]. See also: *Preventing Charity Fraud, Insights+Action*. October 2019. Fraud Advisory Panel, the Charity Commission for England and Wales. UK: HMSO.

[21] P. Reichel. *Global Crime: An Encyclopaedia of Cyber Theft, Weapons Sales, and Other Illegal Activities*. Greenwood Press 2019, at pp.148 – 154. Also: D. Walker, D. Brock and S. T. Ramon. *Faceless Orientated Policing: Traditional Policing Theories are not Adequate in a*

Cyber World. The Police Journal 2006 79(2), 169 – 309. See also: Crime in England and Wales: Additional tables on fraud and cybercrime. Year Ending December 2018. April 25, 2019. UK: HMSO. Available at: <https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenlandandwalesexperimentaltables>. [Accessed 15 April 2020].

[22] Price Waterhouse Coopers. (2020). PwC’s Global Economic Crime and Fraud Survey 2020. [ONLINE] Available at: <https://www.pwc.com/gx/en/services/advisory/forensics/economic-crime-survey.html>. [Accessed 12 April 2020].

[23] Financial Conduct Authority. (2019). Turning Technology against Financial Crime. [ONLINE] Available at: <https://www.fca.org.uk/news/speeches/turning-technology-against-financial-crime>. [Accessed 12 April 2020].

[24] Financial Conduct Authority. (2020). Financial Crime: Analysis of Firms’ Data. [ONLINE] Available at: <https://www.fca.org.uk/publications/research/financial-crime-analysis-firms-data>. [Accessed 12 April 2020]. Note: The FCA ‘Sandbox’ is supporting firms to innovate in RegTech.

[25] W. Barr. *Shell charities and terrorist financing: a sledgehammer to crack a shell?* Tru. L.I. 2017, 31(4), 202-218. [Accessed 12 March 2020].

[26] Organisation for Economic Co-operation and Development (OECD). (2020). Economic and Financial Crime - OECD. [ONLINE] Available at: <https://www.oecd.org/dac/accountable-effective-institutions/efc.htm>. [Accessed 12 April 2020].

[27] You can read these in-depth in Chapter 2, from p.14 – 37. See: The Charities Commission for England and Wales. (2019). Compliance Toolkit: Protecting Charities from Harm. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/677252/Chapter2new.pdf. [Online]. [Accessed 01 April 2020].

[28] K. Raymond Choo. *Politically exposed persons (PEPs): risks and mitigation*. Journal of Money Laundering Control, 2008 Vol. 11 No. 4, pp. 371-387. See: UK national risk assessment of money laundering and terrorist financing. HM Treasury and Home Office. 2017. UK: HMSO. Also: Directives (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018. Official Journal of the European Union, June 19, 2018.

[29] Lack of published statistical data by charities means that evidence can be extrapolated by drawing comparison with financial services because of the parallels in regulatory compliance reporting requirements. See: S. English, and S. Hammond. *Cost of Compliance*. 2018. UK: Thomson Reuters.

[30] The Charities Commission Compliance Toolkit is an online tool that was produced by the Charity Commission and launched in November 2009. It endeavours to assist charity trustees in protecting the charity from potential abuse and harm through assessment and management of risk. The toolkit covers relevant information and compliance tips on terrorism and other financial crime but also is designed to encourage self-monitoring.

[31] Charities Commissions Compliance Toolkit, chapter 2 at p.7.

- [32] Macmillan. (personal communication, June 23, 2020).
- [33] Above note 36. Charities engage with AI from an information perspective, but a wide gap exists between the current paper-based regulatory compliance and any future use of AI.
- [34] Model driven machine executable regulatory reporting TechSprint. FRC, November 20, 2017. <https://www.fca.org.uk/events/techsprints/model-driven-machine-executable-regulatory-reporting-techsprint>. [Online]. [Accessed 22 June 2020].
- [35] Other relevant legislation, for the purposes of charitable organisations, includes; Anti-Terrorism, Crime and Security Act 2006, Counter Terrorism Act 2008, Terrorist Asset Freezing etc. At 2010, Terrorism Prevention and Investigations Measures Act 2011, Protection of Freedoms Act 2012 and the Counter Terrorism and Security Act 2015.
- [36] For a greater discussion see: E. Carrabine et al. *Criminology: A Sociological Introduction*. 3rd Edition. Routledge 2008. Also: M. Deflem (Ed.). *Terrorism and counterterrorism: Criminological Perspectives*. Elsevier 2004. And; E. Mclaughlin. *Terrorism*. 2006. In E. Mclaughlin and J. Muncie (Eds.). *Sage Dictionary of Criminology*. 2nd Edition. Sage 2012.
- [37] See s.1(1) – (5) of the Terrorism Act 2000 as amended by the Terrorism Act 2006 (note s.34) and the Counter-terrorism Act 2008 (note ss.75(1)(2)(a) and 100(5) with s.101(2)); Statutory Instrument 2009/58).
- [38] Governments will need to be vigilant that shell companies and charities are not used to finance terror.
- [39] See also: Council Regulation (EC) No 2580/2001 of 27 December 2001 on Specific Restrictive Measures Directed Against Certain Persons and Entities with a View to Combating Terrorism. Available at: <http://www.legislation.gov.uk/eur/2001/2580/contents#> [Accessed 12 April 2020].
- [40] The Prevent Duty is a legal one, it requires the organization to assess the risk of radicalization in the charity, to develop an action plan to tackle this i.e. reduce that risk, and to train staff to recognise extremism and radicalization, to work with other partners, maintain compliance records and reports, and establish a referral mechanism. The statutory guidance is available online Gov.uk. (2020). Prevent Duty Guidance. UK: HMSO. Available at: <https://www.gov.uk/government/publications/prevent-duty-guidance>. [Accessed 16 April 2020]. See also: The Afghanistan (Asset- Freezing) Regulations 2011 (SI 2011/1893) and The Al-Qaida (Asset-Freezing) Regulations 2011 (SI 2011/2742).
- [41] The Charities Commission for England and Wales. (2019). Compliance Toolkit: Protecting Charities from Harm.
- [42] The UK government suggests that the highest risk, in terms of terror finance, comes from those charities that are small-to-medium sized, recently registered and operate overseas using delivery agents, cash couriers, and aid convoys, at p.104 and 189. See above note 8. FATF. (2018). Anti-money laundering and counter-terrorist financing measures – United Kingdom. Note: see pp.191 – 193 for a discussion on penalties and sanctions for compliance failures. The Office of Financial Sanctions Implementation (OFSI) Guide to Financial Sanctions helps

charities comply with financial sanctions and monetary penalties for financial sanction breaches.

[43] K. T. Smith, M. Smith and K. Wang. *Does brand management of corporate reputation translate into higher market value?* *Journal of Strategic Marketing*. 2010 18:3, pp.201-221. [Accessed 12 April 2020].

[44] These are acronyms for regulatory technology, finance technology and insurance technology. They primarily refer to the automation of regulatory compliance functions but have been broadened out, as they have developed, to refer to the automation of other functions too i.e. digital trading or resolution and legal disputes etc. See above: notes 11 and 12.

[45] K. Harrison and N. Ryder. *The Law Relating to Financial Crime in the U.K.* Routledge 2017. See chapters 2 and 3 for an in-depth introduction to the English approach to terrorist finance and money laundering.

[46] Simser, J. (2008). Money laundering and asset cloaking techniques. *Journal of Money Laundering Control*, 11(1), 15–24.

[47] This process is referred to as ‘smurfing’.

[48] For a discussion on money laundering and electronic money flow see: D. Hopton. *Money Laundering: A Concise Guide for All Business*. Gower 2009, 3.

[49] Financial Action Task Force, Third Mutual Evaluation Report Anti-Money Laundering and Combating the Financing of Terrorism – The United Kingdom of Great Britain and Northern Ireland (Financial Action Task Force: Paris, 2007).

[50] The Commission is funded by the UK government and like Companies House, undertakes the registration process and maintains the register and can also deregister (close down) a charity. Note; charitable trusts are enforced in the name of the Crown by the Attorney General.

[51] The Charity Commission’s approach is set out in detail in its Compliance toolkit, Chapter 1 Module 2 at p.1. See above, note 28.

[52] See above, note 28.

[53] The text of the recommendation highlights the potential for abuse and the need for regulation of the Third Sector; ‘Past and ongoing abuse of the NPO sector by terrorists and terrorist organisations requires countries to adopt measures both: (i) to protect the sector against such abuse, and (ii) to identify and take effective action against those NPOs that either are exploited by, or actively support, terrorists or terrorist organisations.’ FATF. (2015). Best Practices Paper on Combating the Abuse of Non-Profit Organisations (Recommendation 8). In addition, charities (and NPOs) should ‘adopt methods of best practice with respect to financial accounting, verification of program specifics, and development and documentation of administrative, and other forms of control ... use formal financial systems to transfer funds and perform due diligence and auditing functions of partners and field and overseas operations respectively.’

Available at: <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/bpp-combating-abuse-npo.html>. [Accessed 23 April 2020]. See also: Security Council Resolution 1373 (UNSCR 1373).

[54] There is an exaggerated regulatory compliance issue for smaller or inexperienced (new) charities that are run by fewer individuals; excessive pressure can often lead to serious failures.

[55] Consultation for revision to the Code was completed in 2019. Codes that are not legally binding are considered to be ‘soft’ law.

[56] The latest version of the Code, 2018, is published by the Financial Reporting Council seeks to promote ‘a corporate culture that is aligned with the ... purpose ... strategy ... promotes integrity and values diversity.’ FRC. (2018). UK Corporate Governance Code. Available at: <https://www.frc.org.uk/directors/corporate-governance-and-stewardship/uk-corporate-governance-code>. [Accessed 23 April 2020].

[57] R. Gordon, M. Smythe and T. Cornell. *Sanctions Law*. Hart Publishing 2019. Also: M. Happold and P. Eden. *Economic Sanctions and International Law (Studies in International Law)*. Bloomsbury 2019.

[58] Transparency International seek to stop the abuse of power, bribery and secret deals trying to ensure that governments act in the public interest and are not influenced by criminal, financial or other more vested interests. They create a ‘Corruption Perceptions Index’, the latest 2019 highlight corruption hotspots; greater risk for abuse.

[59] See above note 50.

[60] In the case of extreme risks, it may be that the charity ceases to operate in that country or area.

[61] Regulatory sandboxes provide frameworks for creating and testing dynamic and innovate products, technology and a range of business models. The approach to these sandboxes varies across jurisdictions. For a discussion on FinTech and the regulatory sandboxes see; S. Robinson, S. Altkemper and Y. K. Johal. *The regulatory FinTech Sandbox: A Global Overview*. Comp. & Risk 2020, 9(1), 10-14. [Accessed 29 April 2020]. See also: D. Lee Kuo Chuen and R. Deng (Eds.). *Handbook of Blockchain, Digital Finance, and Inclusion, 2017 Volume 1: Cryptocurrency, FinTech, InsurTech, and Regulation*. Singapore: Academic Press, chapter 16.

[62] Charities Commission provides annual charity accounts, a detailed discussion is beyond the scope of this article.

[63] Charities (Protection and Social Investment) Act 2016 extends a range of criminal offences to charities.

[64] Extensive discussion on this matter is beyond the scope of this research.

[65] Homomorphic encryption performs calculations on encrypted information, the difference is that it does not decrypt it first. This makes cloud computing more secure.

References

AI resource centre: IBM. (2020). Mitigating Human Bias in AI.

Barr, W. *Shell charities and terrorist financing: a sledgehammer to crack a shell?* *Tru. L.I.* 2017, 31(4), 202-218.

Bellamy, R. K. E. Et al. *AI Fairness 360: An extensible toolkit for detecting and mitigating algorithmic bias.* *IBM Journal of Research and Development*, vol. 63, no. 4/5, pp. 4:1-4:15, 1 July-Sept. 2019.

Beioley, K. Robots and AI threaten to mediate disputes better than lawyers. (2019). *Financial Times*.

Breen, O. B. *Through the Looking Glass: European Perspectives on Non-Profit Vulnerability, Legitimacy and Regulation.* *Brooklyn Journal of International Law*, Vol. 36, No. 3, pp. 948-991, 2011; UCD Working Papers in Law, Criminology & Socio-Legal Studies Research Paper No. 47/2011.

Carrabine, E. *Criminology: A Sociological Introduction.* 2014, 3rd Edition, Routledge.

Carlisle, D. *FinTech: The Next Frontier.* *Money L.B.* 2017, 249, 8-11 and T. Malloy. *Fine Words.* *Money L.B.* 2007, 141, 1-3.

Charities Commission for England and Wales. (2019). Preventing Charity Cybercrime. Insights + Action. Fraud Advisory Panel. [Online].

Commissioners for Special Purposes of Income Tax v Pemsel [1891] AC 531.

Crime in England and Wales: Additional tables on fraud and cybercrime. Year Ending December 2018. April 25, 2019. UK: HMSO.

Cyber Security Guide for Charities. GCHQ: National Cyber Security Centre. UK: HMSO.

Deflem, M. (Ed.). *Terrorism and counterterrorism: Criminological Perspectives.* 2004, Elsevier.

Directives (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018. Official Journal of the European Union, June 19, 2018.

EMC Education Services. (Ed.). *Data Science and Big Data Analytics: Discovering, Analysing, Visualizing and Presenting Data.* 2015, John Wiley and Sons.

English, S. and Hammond, S. *Cost of Compliance.* 2018, Thomson Reuters.

Financial Action Task Force. Anti-money laundering and counter-terrorist financing measures – United Kingdom. 2018, Fourth Round Mutual Evaluation Report, FATF, Paris.

Financial Action Task Force. Anti-money laundering and counter-terrorist financing measures – United Kingdom. 2018, FATF, Paris.

Financial Action Task Force. Third Mutual Evaluation Report Anti-Money Laundering and Combating the Financing of Terrorism – The United Kingdom of Great Britain and Northern Ireland (Financial Action Task Force: Paris, 2007).

Financial Action Task Force. Best Practices Paper on Combating the Abuse of Non-Profit Organisations (Recommendation 8). 2015, FATF, Paris.

Financial Conduct Authority. Turning Technology against Financial Crime. 2019, FCA.

Financial Conduct Authority. Financial Crime: Analysis of Firms' Data. 2020, FCA.

Fraud Advisory Panel, the Charity Commission for England and Wales. UK: HMSO.

Financial Reporting Council. UK Corporate Governance Code. 2018, FRC.

Gordon, R., Smythe, M. and Cornell, T. *Sanctions Law*. 2019, Hart Publishing.

Gov.uk. *Prevent Duty Guidance*. 2020, HMSO.

Happold, M. and Eden, P. *Economic Sanctions and International Law (Studies in International Law)*. 2019, Bloomsbury 3PL (USA: Hart Publishing).

Harrison, K. and Ryder, N. *The Law Relating to Financial Crime in the U.K.* 2017, Routledge.

Hopton, D. *Money Laundering: A Concise Guide for All Business*. 2009, Gower: Farnham, 3.

Hornle, J. Dispute resolution: digital alternative. June 16, 2014. Law Society Gazette.

Kingston, K. G. *Concealment of Illegally Obtained Assets in Nigeria: Revisiting the Role of the Churches in Money Laundering*. A.J.I.C.L. 2020, 28(1), 106-121.

Lee Kuo Chuen, D. and Deng, R. (Eds.). *Handbook of Blockchain, Digital Finance, and Inclusion, Volume 1: Cryptocurrency, FinTech, InsurTech, and Regulation*. 2017, Singapore Academic Press.

Leary, K. The Verdict Is In: AI Outperforms Human Lawyers in Reviewing Legal Documents. 2020, Futurism.

Long, W. R. M. and Agyekum, J. *European Commission's Public Consultation on Proposed EU Artificial Intelligence Regulatory Framework*. Data Matters. May 2020. [ONLINE].

Mclaughlin, E. and Muncie, J. (Eds.). *Sage Dictionary of Criminology*. 2013, 2nd Edition, Sage.

Model driven machine executable regulatory reporting TechSprint. FRC, November 20, 2017. [Online].

Non-profits. Charitable Giving Statistics, Trends & Data: The Ultimate List of Charity Giving Statistics. 2018. [ONLINE].

P. S.Davies, G. Virgo and E. H. Burn *Equity and Trusts: Text, Cases and Materials*. 2016, Oxford University Press.

Organisation for Economic Co-operation and Development (OECD). (2020). Economic and Financial Crime - OECD. [ONLINE].

Ottavi. A. Shell Corporations and Beneficial Owners. Current Criticalities and Future Developments from a Multilevel Perspective. *Bus. L.R.* 2019, 40(3), 116-123.

Picarda QC, H. *Law and Practice Relating to Charities*. 2010, 4th Ed. UK: Bloomsbury Professional.

Price Waterhouse Coopers. PwC's Global Economic Crime and Fraud Survey 2020.

Raymond Choo, K. Politically exposed persons (PEPs): risks and mitigation. *Journal of Money Laundering Control*, 2008, Vol. 11 No. 4, pp. 371-387.

Reichel, P. *Global Crime: An Encyclopaedia of Cyber Theft, Weapons Sales, and Other Illegal Activities*. 2019, Greenwood Press at pp.148 – 154.

Robinson, S., Altkemper, S. and Johal, Y. K. The regulatory FinTech Sandbox: A Global Overview. *Comp. & Risk* 2020, 9(1), 10-14.

Rossi, F. Building Trust in Artificial Intelligence. *Journal of International Affairs*. 2018, 72(1), pp.127-134.

Sheldon, K. S. *Successful Corporate Fund Raising: Effective Strategies for Today's Non-profits*. Wiley Non-profit Law, Finance and Management Series. 2000, John Wiley & Sons.

Sahota, N. and Ashley, M. *Own the A.I. Revolution: Unlock Your Artificial Intelligence Strategy to Disrupt Your Competition*. 2019, McGraw-Hill Education.

Sahota, N. Will A.I. Put Lawyers Out of Business? 2020. [ONLINE].

Simser, J. Money laundering and asset cloaking techniques. *Journal of Money Laundering Control*. 2008, 11(1), 15–24.

Smith, K. T., Smith, M. and Wang, K. Does brand management of corporate reputation translate into higher market value? *Journal of Strategic Marketing*. 2010, 18:3, pp.201-221.

Security Council Resolution 1373 (UNSCR 1373).

The Charities Commission for England and Wales. Compliance Toolkit: Protecting Charities from Harm. 2019. [Online].

The Afghanistan (Asset- Freezing) Regulations 2011 (SI 2011/1893)

The Al-Qaida (Asset-Freezing) Regulations 2011 (SI 2011/2742).

Third Sector. (2013). Global charitable giving could reach £146bn by 2030, says Charities Aid Foundation report.

UK national risk assessment of money laundering and terrorist financing. HM Treasury and Home Office. 2017. UK:HMSO.

Walker, D., D. Brock, and S. T. Ramon. Faceless Orientated Policing: Traditional Policing Theories are not Adequate in a Cyber World. *The Police Journal*. 2006, 79(2), 169 – 309.

Whalley, M. and Guzelian, C. *The Legal Risk Management Handbook: An International Guide to Protect Your Business from Legal Loss*. 2016, Kogan Page.

Wood, J. This AI outperformed 20 corporate lawyers at legal work. 2020, World Economic Forum.