Technology and tax evasion in the world of finance: an indispensable helping hand or a façade for crime facilitation?

Viksha Ramgulam and Sam Bourton[1]

1. Introduction

Ever since the imposition of the first income tax, individuals have attempted to evade their tax liabilities. Tax evasion involves the non-payment of a tax liability that a taxpayer was legally obligated to pay, usually because relevant information, income and/or assets have been hidden, concealed or misrepresented to tax authorities (OECD 2020; HMRC, 2020a). The motivation to evade taxation appears to be unaffected by the amount of income earned by each individual (Pickhardt, Prinz, 2012) although the very wealthy and the self-employed may be better able to realise this ambition (Alstadsaeter, Johannesen, Zucman, 2019). This is partly because these individuals are better placed to take advantage of the benefits of globalisation, including advances in technology and the increasing mobility of capital (McCracken, 2002). Tax evasion causes substantial losses to government revenues, posing a serious risk to public infrastructure, public services and/or honest taxpayers through their increased burden. Indeed, the European Union (EU) estimates that Member States' revenue losses attributable to international tax evasion amounted to €46 billion in 2016 (European Commission 2019). Domestically, the UK's tax authority, Her Majesty's Revenue and Customs (HMRC), estimates that the revenue losses attributable to tax evasion amounted to £4.6billion in the UK in 2018-19 (HMRC, 2020a). In recent times, international organisations and national revenue authorities have intensified their efforts to combat this financial crime. These efforts have been made in response to an increased public appetite to combat tax evasion, particularly offshore tax evasion, itself prompted by prominent tax evasion scandals involving the concealment of wealth offshore. For instance, in February 2015, it was revealed that HSBC Private Bank (Suisse) had assisted many wealthy clients in evading millions of pounds in tax, including over 1,000 of its UK clients (ICIJ 2015). Further, in April 2016, a leak of documents from the Panamanian law firm Mossack Fonseca, revealed how clients of the firm utilised legal structures and banking secrecy in offshore jurisdictions, to launder money, avoid sanctions and engage in tax minimising activities, including tax evasion (ICIJ 2016).

[1] Bristol Law School, University of the West of England.

Technological innovation has played a pivotal role in the global response to this problem, with systems providing for the automatic exchange of information, such as the Organisation for Economic Cooperation and Development's (OECD), Common Reporting Standard (CRS), revolutionising attempts to combat offshore tax evasion (Pross *et al*, 2017). Moreover, national tax authorities are making increasing use of technology, particularly data mining and analysis tools and methods, vastly improving their ability to detect and investigate tax evasion (Pijnenburg, Kowalczyk, van der Hel-van Dijk, 2017). In this respect, technology is becoming an indispensable helping hand in efforts to combat tax evasion. Indeed, in the UK, since implementing the CRS, HMRC has received 5.67 million records, relating to 3 million UK resident individuals, or entities they control, and since 2010 has raised over £2.9 billion through combatting offshore tax evasion (HMRC, HM Treasury, 2019). Moreover, HMRC's data analysis tool, Connect, plays a pivotal role in instigating 90% of HMRC enquiries (Sanghrajka, 2020), and was estimated to have raised over £4billion by 2019 (HMRC 2016).

On the other hand, there are fears that these efforts could be thwarted by criminals making increased use of technological innovation. For instance, Marian (2013) posits that cryptocurrencies may 'replace tax havens as the weapon-of-choice for tax-evaders', owing to their anonymity and ability to escape taxation, as well as their independence from financial institutions. In addition, technological innovation has spawned new sectors of the economy, such as the sharing economy, which encompasses businesses that provide online marketplaces, such as AirBnB, Uber and Ebay (OECD, 2017). These online marketplaces have enabled sellers to engage in income tax evasion and VAT fraud, with over £1billion lost to VAT fraud and error via these platforms each year (Parliament, 2017c). In this respect, technology may also be an increasingly dangerous façade for crime facilitation, providing assistance to those who seek to illegally escape their tax liabilities.

Accordingly, this chapter seeks to investigate the role of technological innovation in the development of methods used to commit tax evasion, as well as the methods used to detect and respond to this financial crime. In this respect, the chapter will determine whether technological innovation ultimately helps or hinders efforts to combat tax evasion. In furtherance of this aim, the first section investigates the role of technological innovation in assisting tax evaders to conceal information, income and assets from tax authorities to evade their tax liabilities. In particular, this section will focus on the dangers posed by cryptocurrencies in facilitating tax evasion, as well as the difficulties posed by online marketplaces in detecting and addressing tax fraud. The second section will examine the criminal offences used to address these financial

crimes in the UK, while the penultimate section will consider the role of technology in combatting this financial crime. The chapter will conclude by arguing that technological innovation has assisted both those who evade their tax liabilities, as well as those charged with the enforcement of those liabilities. However, greater use of technology could enable tax authorities to stay one step ahead of tax evaders, thwarting their attempts to remain beyond the reach of the law through technological advancement. In particular, the chapter discusses the possibilities offered by increased use of blockchain technology.

2. Technology - a façade for crime facilitation?

The legal world which could formerly merely be described as a dilettante in the subject of technology is now having to adapt itself to concepts such as Bitcoin in order to keep up with the financial industry (Srivastava *et al*, 2018). These new concepts are creating what can only be described as 'justifiable and qualified concerns' over a potential rise in tax evasion (Weber, Baisch, 2018). New innovations such as Paypal, Revolut, Monzo and Bitcoin therefore call for an adaptation on the rules and regulations with regards to tax evasion. Brummer and Gorfine (2014), notably, make an interesting case for further regulation, citing Fintech's disruptive characteristics as requiring an equally innovative regulatory model and rulemaking process to tackle its adverse effects. Indeed, they support the view that FinTech disrupts fundamental principles of existing regulatory approaches and thereby 'requires fresh thinking' to maximise the effectiveness of its regulation. This section aims to discuss the impact of globalisation on efforts to combat tax evasion, with a focus on technology as a complex modern component to effective law enforcement, as well as an accessory to tax evaders. In particular, the following section will discuss the challenges posed by e-commerce and cryptocurrencies.

E-commerce and VAT evasion

The demographic of the economy is moving towards gig and sharing economies (Volkin, 2020; Economist 2013), defined as states of affairs with considerable legal persons providing resources on flexible terms on a global scale. Indeed, gig economies relate to the increase in flexitime work (Bennett, 2020), whilst the sharing economies refer to asset-sharing, for instance, letting property or crowdfunding (Asquith, 2020). With commercial exploitation on the rise, niche items such as 'Vintage designer' are being sold by small businesses on million-dollar platforms such as Etsy, Depop, and Poshmark (O'Flaherty, 2019; Indvik, Abboud, 2020). Worryingly, such items are acquiring the same uniqueness and subjectivity as art (Hufnagel, King 2020), becoming headaches for authorities to trace concealed, misrepresented

and omitted accounts of money (Hyde, Greene 2020). Indeed, as the Fifth Money Laundering Directive (5MLD)[2] is catering to art intermediaries and other high value dealers, more risks are now emerging from these small enterprises. Such niche retail businesses, takeaways and hospitality have in fact been identified as high-risk industries for tax evasion (HMRC, 2020c). Indeed, despite HMRC's far-reaching powers, such as those contained in Schedule 23 of the Finance Act 2011, it cannot identify and therefore investigate these unregistered businesses, consequently losing £1.5bn in VAT revenue in 2016 (Parliament 2017c).

In fact, eBay and Amazon have been accused of 'profiting from VAT evaders' with Haines (2017) explaining how their commission received from transactions is encouraging them to condone illicit activities. In such situations, making corporations fiscally responsible could be a remedy, especially virtual marketplaces. Taxes of independent retailers are now deducted through virtual marketplaces, demonstrating the UK's efforts to fight tax evasion and third party facilitation, by tackling hidden economies (Parliament, 2017b; Beetham, Cape, 2018). Since then, Amazon has demonstrated compliance by implementing a built-in VAT returns service to its Seller Central account (Amazon, 2019; Asquith, 2020). This reinforces the endless capabilities of technology and how better knowledge surrounding it would lead to its effective use, ultimately leading to tax evasion prevention. In fact, such initiatives could benefit corporation by allowing them to undertake responsibility vis-à-vis independent retailers in their desired cost-efficient way, without the rigid instructions that often accompany compliance regulations (Highfield, Evans, Walpole, 2019).

Moreover, organisations such as RAVAS (Retailers Against Vat Abuse Schemes) and VATFraud are uncovering tax fraud before HMRC (Haines, 2017; Parliament, 2017a), denoting HMRC's lack of specialisation in technology. More importantly, it highlights technological innovation as a beneficial, but also, destructive tool to tax evasion prevention, as well as the subsequent need for authorities to recognise the role of technology and take responsibility to make regulations capable of responding to both technological and traditional methods of tax fraud and evasion. Offences involving VAT evasion, excise duties and e-commerce, albeit not evolving in substance, are becoming more prevalent with technology and thus, to be identified and prevented effectively, monitoring technology as well as reforming legislation is required

[2] Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 Amending Directive (EU) 2015/849 on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing, and Amending Directives 2009/138/EC and 2013/36/EU [2018] OJ L 156/43

Cryptocurrency creating new realms for TE

There will be no information to exchange and regulate by financial institutions for the purposes of tax returns if it is stored as a blockchain, as cryptocurrency usually is, making it harder to maintain effective tax evasion prevention. 5MLD defined cryptocurrencies broadly as 'a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred stored and traded electronically'. Such an attempt was crucial considering cryptocurrency shares mutual characteristics with lower-tax jurisdictions, namely, the ability to enable individuals to anonymously conceal income from tax authorities (Marian, 2013). However, cryptocurrencies are 'super tax havens' as they add an additional layer of anonymity by operating independently from regulated financial institutions (Böhme *et* al, 2015). Therefore, cryptocurrencies have become more attractive for tax evasion purposes than tax havens, demonstrating the role of technological innovation in creating new virtual realms for tax evasion offences (Brown, 2016).

This concept therefore strongly defies recent initiatives to combat financial crime, such as the exchange of information to implement and promote transparency through beneficial ownership and the EU's Fourth Money Laundering Directive(4MLD).[3] The 5MLD has sought to remedy this situation, together with the UK's Money Laundering and Terrorist Financing (Amendment) Regulations (MLR) 2019, SI 2019/1511. Article 1(2)(d) of 5MLD has attempted to combat the illicit use of virtual assets by labelling virtual currency exchanges (legal persons providing the trade between fiat and virtual currencies) and custodian wallet providers (legal persons supplying services relating to the safeguard of private cryptographic keys) as 'obliged entities.' This makes them subject to identical CFT/AML regulations as financial institutions per 4AMLD.

The UK has implemented the EU's anti-money laundering directives post-Brexit with The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, SI 2017/692 (MLR) 2017 implementing the 4MLD, and the MLR 2019 implementing 5MLD. Considering Brexit, this denotes the UK's intrinsic efforts to combat tax evasion notwithstanding its lack of continued participation in the EU (Turner, Bainbridge,

[3] Directive 2015/849 of 20 May 2015 On the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing [2015] OJ L141/73

2018). However, despite the Regulations increasing the scope of the regulated sector for the purposes of anti-money laundering requirements to encompass cryptoasset exchange providers and custodian wallet providers, the UK's efforts remain lacklustre considering the fast pace of technology and the inadequate constructive advancements regarding the regulation of crypto-assets. In light of the growing use of technology by tax evaders to conceal income or assets from tax authorities, it is imperative that the legal framework is able to withstand the challenges presented by technological innovation. Accordingly, the following section examines the offences pertaining to tax evasion in the UK, considering whether the UK's tax legislation remains fit for purpose in light of technological innovation.

3. Tax Evasion Offences

Tax evasion offences will form the focus of this section, followed by an analysis of selected areas that have been impacted by technological innovation. Statutory and common law offences will be evaluated, and the shared key legal requirements of these offences will be discussed concomitantly.

Income tax evasion

The offence contained in s. 106A of Taxes Management Act 1970, relating to income tax refers to the 'fraudulent evasion' of money levied on wealth (money, property or services) resulting from earnings from employment, dividends, royalties, interest or self-employment. s.106B, s.106C and s.106D Taxes Management Act 1970 contain strict liability offences such as the failure to provide notice of liability to income and capital gains tax, and failure to deliver and to make accurate returns regarding offshore income, assets, or activities respectively. Whilst it has been perceived as being too harsh and limited in scope, this offence being strict liability, it could in fact remediate the unwarranted loopholes caused by technological innovation when combined with the problematic test of dishonesty in English Law, discussed further below. It irrefutably eases convictions because it removes the mens rea and its drawbacks immediately from the equation, and as such is deemed very effective (Bourton, 2018). However, the offence is limited in scope, applying only to income, assets, or activities in excess of the threshold amount, which is currently £25,000 of potential lost tax revenue per year, and which are not reportable under the CRS (Taxes Management Act 1970 (Specified Threshold Amount) Regulations 2017, SI 2017/988).

The IR35 and Regtech

Notable reform regarding income tax includes the IR35 rules to off-payroll workers taking effect in April 2021, as per s.38 of the Finance Act 2018 (HMRC 2019c; Groom, 2020). This has been implemented following individuals evading taxes through self-assessment by claiming to be independent contractors to large companies. The reform thus prescribes that personal service companies be taxed equivalently to the Pay As You Earn (PAYE) scheme in instances where but for the title of 'personal service company', the individual would be an employee of the company rather than a contractor (Hyde, Greene, 2020). This reform aims at shaping the law to put the onus of these individuals on their large corporate employers as opposed to the HMRC. A failure to determine a genuine contractor from an employee through the 'but for' test mentioned could lead to such companies being liable for unpaid taxes. This option, as opposed to simply prosecuting corporates through 'failure to prevent' offence (explained below) thereby by-passes any escaped liability which could have occurred with the 'Too Big to Jail'(TBTJ) policy. Instead, no resources are wasted from aiming to prosecute large corporates and the HMRC obtains its tax revenue owed, thereby creating an effective tax evasion prevention structure.

The IR35 rules demonstrate the role of technological innovation in improving tax collection, as RegTech will be a prerequisite for most medium and large enterprises to be equipped to do this task (Barberis, Arner, Buckley, 2019; Deloitte, 2020). This leads to the encouragement of rigid tax risk assessment and compliance, and even engages companies' inclinations towards corporate social responsibility, paving the way to reinforcing the latter. Furthermore, it reduces the risk of falsification of documents through technology as the documents are filed through the large corporates. With time, this may transition into a more 'intrinsic motivation to pay taxes', also known as tax morale, which is deemed to be essential for effective tax administration (OECD, 2019; Luttmer, Singhal, 2014).

Evasion of VAT and Customs and Excise Duties

VAT evasion relates to the act of deliberately not paying VAT on the supply of goods and services, having taken possession of goods from the EU and outside the EU. This form of evasion is criminalised under the Value Added Tax Act (VATA) 1994, s72(1).

Another form of tax evasion on goods relates to the evasion of Customs and Excise duties under the Customs & Excise Management Act (CEMA) 1979. s.170(1) provides for offences related to knowingly acquiring or being knowingly concerned in a transaction involving a commodity under the Act, with intent to defraud the public of such duties. As per *R v Neal*

[1983] 77 Cr App R 283 at 287, s170(1) CEMA has an exceptionally wide ambit so that it is a 'catch all provision,' as it relates to any 'fraudulent evasion' or 'attempt,' and also implicates anyone 'knowingly concerned' in the evasion, thus also serving as a coercing mechanism to prevent individuals from even attempting or facilitating such an offence.

Providing False Documents and Information to HMRC

These offences, contained in CEMA 1979, s.167(1), concern making false declarations to HMRC and counterfeiting documents. Technology has inarguably enabled the falsification of documents with hacking, facial 'deep fakes' recognition technology (Hendrikse, 2020). The simple falsification of documents is becoming more widespread, making this offence particularly useful in the fight against tax evasion. For both offences, the prosecution must prove that the documents were not authentic in a 'material particular.' As per *R v Cross* [1987] Crim LR 43, this is up to the judge to establish rather than the jury. This is particularly effective to tax evasion prevention in situations where establishing the factual context of the offence is complex. Technological innovation complicates situational facts, thereby requiring the determination of the law and the capacity to innovate which the judge can more effectively provide (Dari-Mattiaccia, B Deffains, B Lovat, 2011). Knowledge or recklessness as to whether the information is true is essential for this offence, see *R v G and another* [2003] UKHL 50. As per *Page* [1996] Crim LR 821, a high level of negligence could suffice. This is particularly relevant to cases of technological innovation, since individuals cannot necessarily be acquitted for wilful blindness, but instead, must have taken appropriate measures for this to occur.

The Corporate Offences of Failure to Prevent Tax Evasion

Part 3 of the Criminal Finances Act 2017 prescribes a partnership or company guilty of a criminal offence if a person employed or otherwise having acted for, and on behalf of, the company is knowingly concerned in a tax offence committed in the UK, s.45, or abroad, s.46. The company is criminally liable if they cannot provide the defence of having taken proportionate measures in cases of suspicious activity. Again, 'Nelsonian dishonesty', the act of turning a 'blind eye' to behaviour such as tax evasion, is not tolerated (Hyde, Greene, 2020). This offence has set the tone for tax evasion prevention by bypassing the identification doctrine, which is used to attribute liability to corporations for criminal offences. As per *Tesco Supermarkets Ltd v Nattrass* [1972] AC 153, the identification doctrine is described as the process of identifying the natural person(s) acting as the directing will and mind of a company,

for whose actions liability can be attributed to the company itself. The strict liability offences remedy the problems associated with the doctrine, specifically, an inability to establish the relevant *mens rea* on the part of individuals identified as 'directing minds', often because these individuals will obscure their involvement in the offence by delegating actions to junior employees and failing to record information (Ministry of Justice 2017; HMRC 2017). As such, the new offences prevent such discrepancies by only requiring the fact that an individual working for or on behalf of a company facilitated this offence and that the company did not have the reasonable procedures in place to cater to such occurrences. Therefore, this puts the onus on companies to adopt reasonable procedures to prevent the facilitation of tax evasion and thereby act more responsibly. This in turn should increase tax morale, thereby increasing tax compliance. In this way, reforming criminal legislation seems fair and proportional to the ever-evolving risks posed by tax evasion and prima facie seems not only highly effective, but also socially and economically desirable.

Common law offence: Cheating the public revenue

After cheating was abolished by the Theft Act 1968, it survived partly through 'cheating the public revenue' (Ormerod, Laird, 2015), referred to in *R v Less, The Times,* March 30, 1993, as 'conduct intended to dishonestly and deliberately deprive HMRC of tax that would otherwise be due.' As per *R v Hudson* [1956] 2 QB 252, an individual may be convicted of tax evasion if the prosecution can show that the defendant has made a false statement with the intent to defraud the HMRC. This can take the form of a positive act or failure to act. A requirement, however, is dishonest intent to evade tax or Nelsonian blindness to someone else stealing from the HMRC; recklessness is not sufficient for conviction. Nonetheless, as Ormerod (1998, p.630) states, the scope of this offence is so broad that dishonesty is often the 'only live issue' at trial. Indeed, the argument in *Mavji* [1987] 1 WLR 1388 over the requirement of deception was rejected. Ormerod notes that the broad scope of the offence has led to concerns over the potential criminalisation of failed tax avoidance schemes, as in *R v Charlton and Ors* [1996] STC 1418. As Yorke (2017, p.16) explains, 'what turns tax planning into tax evasion is merely the added ingredient of dishonesty.'

With regards to technological innovation, it can be argued that the wide ambit of this offence, requiring mere dishonesty, caters to innovations unforeseen by the law, especially in the case of complex case facts encompassing technology, as it removes complex subjective elements from the equation enabling the jury to identify causality and dishonesty more easily. Indeed,

this is especially the case considering the new methods of tax arbitrage in light of technology (Yeoh, 2018). Tax arbitrage often involves profiting on the thin line between tax avoidance and tax evasion (Marjit, Seidel, Thum, 2017), explained further below. It is noteworthy to point out that the blurred line between these two activities could, however, also be problematic considering that the Rule of Law requires the law to be certain, proportionate and reasonable. It sparks the question of whether if someone thought they were avoiding tax and acting lawfully, should they be prosecuted at all. This could cause a snowball effect in terms of uncertainty for the Rule of Law. Nonetheless, technological innovation has advanced to previously unthinkable extents and, in this way, this offence is highly effective, acting as a buffer to any prospective technology that could be used to facilitate tax evasion.

Key elements of the offences

Knowingly concerned

A common denominator of several tax offences, is the requirement of being 'knowingly concerned'. This refers to having dishonest knowledge as per *R v Montila* [2004] UKHL 50 - exceeding mere suspicion - and actual involvement in their own or someone else's fraudulent evasion (Harrison, Ryder, 2017). In this instance, the knowingly concerned element intends to capture enablers as well as evaders and thus serve as strong deterrent to tax evasion. Considering the 14,000 enablers uncovered by the Panama Papers, many of whom were based in the UK, this could be a useful tool in the fight against tax evasion (European Parliament, 2017). Indeed, these institutions are often hidden in plain sight, as exemplified by the HSBC case, whereby the bank was a regulated financial institution yet acted as an enabler of tax evasion (ICIJ, 2015).

Moreover, this requirement results in a significantly reduced extent of illegal tax arbitrage, such as the recent German Cum/Ex scandal (Segal, 2020). This method involves multiple counterparties (in this instance in the finance and banking industry) with differing degrees of knowledge over transactions which aim at exploiting one singular loophole regarding dividend payments, which allow them to claim the same tax rebate (Seddon *et al*, 2020). Subsequently, paying greater attention to enablers could lead to enforcement uncovering individuals who could actually be tax evaders. In this way, benefits to this aspect are twofold, as it catches both enablers and potentially evaders. Moreover, there is a significant likelihood of detection in this area owing to its imperfect concealment technology (Marjit, Seidel, Thum, 2017). In this way, more individuals are caught causing a stronger deterrent effect. Accordingly, the 'knowingly

concerned' doctrine establishes an increased scope for liability and is thus inarguably a competent measure to combat tax evasion fuelled by technological innovation.

Dishonesty

Most tax evasion offences require mens rea, and this is usually encompasses an assessment of whether the offender acted dishonestly. The term dishonesty lacks statutory definition, thereby requiring interpretation. However, as Yorke (2017, p.16) explains, the judiciary hold the view that they 'must not attempt to define dishonesty', as 'the act of dishonesty should be for the jury to single-handedly deliberate according to the present-day standards of the ordinary reasonable and honest man or woman.' Indeed, with the exception of the strict liability offence, it is a crucial common element of both the nature and definition of many tax evasion offences (Bourton, 2018). However, the identification of dishonesty in the assessment of criminal behaviour for the purposes of distinguishing illicit and licit non-compliance remains difficult. Salter (2002) found that 'was this dishonest?' was easier for a jury to answer than 'was this fraudulent'. However, as a general rule, juries are unlikely to have shared perceptions of dishonesty, leading to inconsistency in the criminal law, and may find it difficult determine whether a defendant has been dishonest when dealing with unfamiliar contexts, of which tax evasion cases may be a prime example (Ormerod, 1998).

In *R v Barton and Booth* [2020] EWCA Crim 575, the judge directed the jury based on the test in *Ivey v Genting Casinos (UK) Ltd t/a Crockfords* [2017] UKSC 67 of dishonesty as opposed to the test in *R v Ghosh* [1982] 2 All ER 689. The line of thought of the Supreme Court in *Ivey* regarding the adequate standard of dishonesty was until then obiter dicta, and therefore not legally binding. In Ivey, Lord Hughes previously cited concerns with *Ghosh*'s subjective limb potentially excusing a defendant's liability owing to their 'warped' sense of dishonesty. With the *Barton case* asserting *Ivey* as the correct test for dishonesty in criminal cases mirroring the test for civil matters in *Barlow Clowes International Ltd v Eurotrust International Ltd* [2005] UKPC 37, the issue of excessive subjective contextual variables is somewhat redeemed. Indeed, this test now means that for dishonesty to be found by a jury, as part of their fact-finding duty, they need to be aware of the defendant's knowledge of the situation and then apply the objective test of whether an ordinary reasonable person would believe that what he did was dishonest (Ormerod, Laird, 2020).

Nonetheless, issues in the context of adding advanced technology such as blockchain technology to highly technical offences requiring evidence of causality between the knowingly

concerned and subsequent omission, concealment, or misrepresentation of funds could dilute the application of dishonesty. Indeed, with no constants such as specific definitions or structure to go by, the added subjective ingredient of dishonesty does not facilitate trial proceedings. Moreover, technology in the form of nontraceable and non-identifiable forms of communication such as the dark web, makes it extremely hard to prove the causal link in distinguishing intent from a failed attempt at tax avoidance, or worse, a mere accident. However, this could also make the process easier in the unlikely event that there is proof for the jury of such modes of communication, to thereby assume dishonesty. Considering the dangers of the dark web, this would only serve to be effective in the fight against tax evasion. However, if juries assume that the use of cryptocurrency means that the individual is guilty, this could be a limitation to the effectiveness against tax evasion prevention as an incorrect assumption would render the prosecution disproportional and unfair. Concerns have been raised over lay jurors not only having to consider modern commercial transactions and technical business regulations with all the relevant circumstantial evidence, but also requiring knowledge of advanced technology mirroring that of the evaders (Jordanoska, 2017). Thus, technology can adversely affect dishonesty in substance. It could cause a clouded judgment, thereby negatively affecting the rule of law and simultaneously effective tax evasion prevention.

Conclusion

Whilst technological innovation does not appear to cause new problems for tax legislation, it exacerbates existing ones. Now that it has made the boundaries across countries virtually inexistent, governments and regulators need to make sure laws are able to adapt so that tax evaders cannot escape liability. It has been observed that issues seem to stem from a lack of transparency, leading to the conclusion that cooperation and communication amongst individuals, financial and legal institutions, and nations has never been so essential. Nevertheless, technological innovation may also present new opportunities for tax authorities to investigate and enforce these offences in a manner previously unthinkable. The next section provides a selected overview of the use of technological innovation in combatting tax evasion in the UK, highlighting the benefits to be derived by tax authorities.

4. Technology - An Indispensable Helping Hand?

The digital revolution has opened unprecedented modes of commercial exploitation with wealth never travelling so far, so fast, and so much (Asquith, 2020). With tax crimes

incrementally increasing, Bentley suggests that enforcement is instrumental, perhaps even more so than legislation (Bentley, 2020). He adds that its soft power and ability to lead disruptive tendencies, such as dynamic changes in an economic landscape, allows for an effective and rapid recovery from a situation caused by technological innovation. Indeed, legislation and reform notoriously have political, economic, and socially motivated time lags which are sufficiently long to cause lasting damage in these situations (Gentle, Spinks, Omer, 2019). Contrastingly, enforcement has a paternalistic nature, meaning that it refers to imposing concrete on-demand positive or negative actions on the population. This can remedy loopholes facilitated by technological innovation swiftly, which legislation can reinforce more permanently in due time where required. It is noteworthy that critics such as de la Feria (2020) believe that current taxation collection and regulation methods are more curative than preventive with the government opting for revenue-maximisation from honest businesses to compensate for the tax gap rather than combatting the fraud directly. Indeed, this can be exemplified particularly by the TBTJ mentality which will be discussed further in this section.

Tax evasion is generally investigated by HMRC or by the National Crime Agency (NCA) in England and Wales subject to the safeguards, in the Police and Criminal Evidence Act (PACE) 1984 and prosecuted by the Specialist Fraud Division of the Crown Prosecution Service (CPS). Northern Ireland and Scotland also have legislation mirroring PACE. Where offences occur elsewhere as offshore tax evasion offences, they will be investigated by the HMRC, Serious Fraud Office (SFO) or NCA, and prosecuted by the SFO or CPS. In fact, the powers of the HMRC are derived from PACE 1984 whilst that of the NCA are from the Crime and Courts Act 2013 and the Proceeds of Crime Act 2002. This section seeks to assess the current tax evasion prevention regime by identifying and critically analysing the stages of enforcement: routine detection of tax evasion, targeted investigations, and prosecutions. Ultimately, this chapter will make the case for the standardisation of technology both in its use and understanding, considering how a lack thereof can be detrimental to the fight against tax evasion.

Detection, Investigation and Technology

The Connect Database

Technology plays a crucial role in the stages of routine detection. The Connect database is a notable example of big data technology, and works as a data mining tool sifting through vast quantities of unrelated data including, online SAR reports, and records held by the Land

Registry and Driver and Vehicle Licensing Agency (DVLA). This automated fraud detection tool enables the tracking down of a suspect's digital footprint, made to appear legitimate on paper, and extrapolates and identifies relationships between individuals, companies, and property (Leighton-Daly, 2019). This enables HMRC to detect discrepancies between an individual's reported and actual income, assets and activities. In fact, the HMRC is in search of a similar tool which could uphold intelligence-gathering techniques to identify, assemble and link crypto transactions back to crypto-asset service providers (HMRC, 2020b).

Despite HMRC having practical limitations such as mandatory full disclosure to the courts, *R (Hart and others) v The Crown Court at Blackfriars and HMRC* [2017] EWCA 3091, it has a wide array of powers including information gathering powers, the ability to search and arrest persons, and recover illicit assets (HMRC, 2019a). HMRC uses it data-gathering powers in Schedule 23 to the Finance Act 2011 to extract information from third-parties, such as online platforms like eBay, detecting VAT evasion and other undeclared revenue and capital gains (Palmer, 2015). It even extracts information from airline companies to identify red flags designating the true representation of individuals' or legal persons' actual lifestyles and situations (Parker, 2019). Accordingly, the Connect database's intrusive surveillance powers delve deeper into tax evasion prevention, by-passing any potential clandestine communication such as untraceable telecommunication via the dark web (Leighton-Daly, 2019). Moreover, it creates smooth transitions between the stages of detection, investigation and prosecution owing to it providing centralised exchange of information, thus creating cost and time efficiency for more effective tax evasion prevention. In fact, the Connect database has proved to surpass itself as a return on investment, costing £80m and providing a return of at least £3bn in government revenue (Rigney, 2016; HMRC 2016).

The Common Reporting Standard and Beneficial Ownership Registers

Nonetheless, there is room for improvement. As always, technological innovation and globalisation cause limitations (Zucman, 2014). Connect can easily investigate multiple people, relationships and transactions in the UK owing to the copious amounts of information HMRC is able to obtain onshore. However, HMRC is often unable to access information relating to income or assets held by individuals in offshore jurisdictions. Accordingly, the UK has implemented the OECD's CRS, which provides for the automatic exchange of information for tax purposes between participating jurisdictions (OECD, 2014). Following the release of the CRS, 49 jurisdictions, including the UK, committed to undertaking the automatic exchange

of information in 2017, and 51 jurisdictions committed to undertaking the first exchanges in 2018 (OECD, 2019a). The UK implemented the CRS via the International Tax Compliance Regulations 2015, SI 2015/878. The information HMRC receives via the CRS is fed into the Connect database (Rigney, 2016). In the UK, since implementing the CRS, HMRC has received 5.67 million records, relating to 3 million UK resident individuals, or entities they control, and since 2010 has raised over £2.9 billion through combatting offshore tax evasion (HMRC, HM Treasury 2019). It is clear that the implementation of the CRS in the UK has led to the collection of substantial amounts of revenue, likely in excess of initial predictions of £75 million to £270 million annually (HMRC, 2015).

The UK has also implemented beneficial ownership registers, as required by 4MLD and 5MLD. It introduced the Persons with Significant Control Register, via the Small Business, Enterprise and Employment Act 2015, s.81, Schedule 3, amending the Companies Act 2006, to identify the natural persons who own or control companies. In addition, the UK introduced a register of the beneficial owners of trusts in the MLR 2017, Part 5, and is currently consulting on the introduction of a beneficial ownership register of overseas entities that own land or real property in the UK (Department for BEIS, 2018). These registers will provide authorities with previously inaccessible information on the ultimate owners of legal entities and structures, which, due to their potentially opaque nature, may be used to evade taxation, hence the need for transparency (Meads, Jarvis, 2014). Accordingly, the registers are considered to be highly valuable in identifying those responsible for financial crimes, including tax evasion.[4] However, the UK's registers currently suffer from deficiencies, in terms of the lack of adequate verification mechanisms for information submitted for inclusion in the register, as well as the lack of effective enforcement of these requirements (Virgo, 2019).

The automatic exchange of tax information, as well as the centralised collection of beneficial ownership information, has been made possible by technological innovation. This is because technology is essential to ensure the fast and standardised transmission of information by financial institutions and responsible authorities, as well as the safe storage of vast amounts of personal data. However, the use of technology to collect vast amounts of personal data has been persistently questioned by commentators, such as Noseda, who questions the compatibility of such measures with rights to privacy and data protection and raises the issue of harm being caused to individuals owing to data breaches through hacking and other cybercrimes (Noseda,

[4] Most UK LEAs believe the Persons with Significant Control Register has had a positive impact in combatting financial crime, see, Department for BEIS (2019), at p.34.

2017). As will be discussed below, further use could be made of technology to address these risks.

An evaluation of investigation-centric instruments

Concerning the investigation process, there remains the question of whether legislative devices have become too obsolete owing to technological innovation. Search warrants are mainly issued under s.8 of PACE 1984. The Law Commission (2018), released a report containing reform proposals listing the latter as convoluted, lacking in consistency, too expensive but more importantly obsolete to the point where there was complete disregard to modern-day criminal activity being largely digital and globalised. The court has tried to take heed of this in *Royal College of Nursing v Department of Health and Social Security* [1981] AC 800, stating that statutory interpretation may and should account for technological innovation. However, considering not all statutory language provides such a flexible and permissive ambit, this solution can only be transitory. Indeed, with evidence now becoming virtual (electronic data), this raises abstract questions regarding seizing material as per *R (Business Energy Solutions Ltd) v Preston Crown Court* [2018] EWHC 1534. As a matter of transition, the court can step in efficiently to fulfil its discretion, but with regards to sustainability, as technology develops further, it will become increasingly difficult for the courts to deliberate on such abstract issues. Indeed, such problems with the law of evidence are not conducive to tax evasion law enforcement: they would not only cause time lags in deliberations and uncertainty, opening the floodgates, but also acquittals solely based off technical deliberations.

Prosecution and technology

Owing to resource limitations, HMRC only refers cases for prosecution where 'the conduct involved is such that only a criminal sanction is appropriate' to their discretion (HMRC, 2019b). Other sanctions include civil penalties. However, following the HSBC (Suisse) scandal, HMRC were tasked with 'increasing prosecutions of 'serious and complex tax crime, focusing particularly on wealthy individuals and corporates' (Parliament, 2016, p.43). Since 2013, HMRC has largely achieved its annual goals, with 1007 prosecutions being brought forward in 2018 (Tax Journal, 2019). The Tax Journal credits compliance from 'online platforms' and Connect to this success, as well as contemporary data mining methods by innovative technology.

Technological innovation inarguably has had a part to play in HMRC's success. The ubiquity of digitalisation itself has led to all-round cost and time efficiency. However, assessing the

extent to which the prosecutions were a success owing to technology is difficult, considering the variable factors possibly involved. Irrespective of its current and past successes, one should not underestimate its efficacy to prove its worth in the foreseeable future. As a recognised pillar of the rapidly-evolving economic landscape, it is irrefutably bringing an increased 'appetite and stamina' in the fight against tax evasion (Tax Journal, 2019).

The influence of technology on Deferred Prosecution Agreements (DPAs)

Entrenched by Schedule 17 of the Crime and Courts Act (CCA) 2013, DPAs are a solution found by the courts in response to criminal offences relating to fraud and dishonesty committed by corporations. They are used in the enforcement of the corporate failure to prevent offence whereby a company thinks that it may have committed tax evasion under s.45 or s.46 of the Criminal Finances Act 2017, but it is not considered to be in the public interest to prosecute (Srivastava *et al*, 2018). The inception of DPAs has been based upon the reluctance of authorities to impose criminal sanctions on 'systematically important' institutions such as banks, which are pillars of the economy (Werle, 2018), fearing negative impacts on the latter as well as 'innocent employees, suppliers and local community' (Milford, 2017). This ideology has been named 'Too Big to Jail' (TBTJ) (Hardouin, 2017). A DPA is an agreement whereby corporate bodies pledge to help the prosecution satisfactorily in return for not giving effect to a formal prosecution later. The satisfactory aspect here relates to benefitting from 'openness' from the offender and transparency to uncover more circumstantial evidence as well as a pledge not to reoffend, hence why self-reporting as a preliminary step to a DPA is preferred. Indeed, this shows a willingness for genuine cooperation, although is not essential, as demonstrated by *Serious Fraud Office v Rolls-Royce Plc and Another* [2017] Lloyd's Rep. FC 249.

Technology can however corrode the aim and process of DPAs. Tech giants such as, Amazon, Facebook, Google, and Apple, are known for their inventive tax avoidance methods (European Parliament, 2016). At the outset, one loophole to DPAs could be a replica of profit-shifting in theory: tech firms could easily alter or send evidence to subsidiaries or colluders in different jurisdictions, especially digital evidence such as intellectual property, to escape liability. Worse, it could be saved virtually or deleted instead of being handed to the authorities. Companies could then mislead authorities by, for instance sending them in the wrong direction of investigation, falsely implanting innocent errors in transaction or even just burying regulatory bodies in mounds of paperwork. Self-reporting in this way, just like self-assessment, can be a defeatist modus operandi in the fight against tax evasion and give regulators and

lawmakers a false sense of accomplishment. Fortunately, monitoring technology can not only counter any wrongdoing, but also upholds authorities as watchdogs regarding any subsidiaries (Srivastava *et al* 2019). Moreover, it can assert transparency required for some firms to prove their innocence and authenticity. In fact, technology has been found to be compatible with DPAs and law enforcement in general.

Interestingly, the use of technological innovation in a domestic criminal case was pioneered by the SFO in *Serious Fraud Office v Rolls-Royce Plc and Another* [2017] Lloyd's Rep. FC 249. Reviewing hundreds of thousands of documents daily, the technology used aimed to remove any Legally Professional Privileged documents, reducing 2 years' worth of work for Independent Counsel into a few months' worth (de Silva, 2018). Such technology could thus promote efficiency, as well as counter misleading information or other attempted shams. Technology in this instance was praised for saving considerable time and cost. In fact, the SFO has since then acquired OpenText Axcelerate, a technology allowing them to operate more efficiently (OpenText, 2018). This resonates with the argument made throughout this chapter that technological innovation is not a solution but it will assist in ensuring compliance and maximising the collection of revenue.

Conclusion

This section demonstrated how technology's understanding and usage is a pre-requisite to modern law enforcement. A lack thereof would only serve to exacerbate the repercussions that result from the use of obsolete laws and methods. Indeed, unfair and disproportionate acquittals would inevitably corrupt the whole process leading up to trial making all efforts at tax evasion prevention futile. The rectification of the enforcement identified inarguably requires extensive efforts and resources. They are, however, key to the fight against tax evasion. Better use of technology on the part of evaders would be nefarious to tax revenue in the long run, not only in terms of escaping liability but also because this would disrupt the deterrent effect of enforcement action, which could lead to an exponential increase in this financial crime.

5. Technological Innovation - An Indispensable Helping Hand or a Façade for Crime Facilitation?

Despite a seemingly robust system in place for TE prevention, a subsequent complacent stance would be ineffective at best and nefarious at worst. Indeed, de la Feria (2020) has observed a rising preference for current tax fraud management approach rather than tax fraud suppression, the former being defined as an enforcement regime overseeing revenue costs of tax frauds

efficiently as opposed to the latter which imposes stricter anti-fraud sanctions as an aim to combat tax evasion. In fact, this tax fraud management approach puts undue strain on companies; in a bid to compensate for evaders, these companies incur increased corporate compliance costs and taxes. The recurring theme perceived throughout this study is that technology is what we make of it: it aids tax evasion prevention if used efficiently and if not, it aids the abettor. Whilst technological innovation's function is to assist rather than be a global independent solution, it is indispensable to effective tax evasion prevention. Moreover, it can assist in supressing, rather than managing tax evasion and fraud.

This section seeks to recommend the approach the law should take towards individuals and corporates who evade taxation in light of technological innovation. Ultimately, this chapter will call for reform. Precisely, it will make the case for big data technology merged with blockchain technology as an effective tool, and the need for authorities to retain their paternalistic leverage over profit-maximising firms to combat tax evasion.

An assessment of the prevention of tax evasion in light of technological innovation

Technological innovation is more problematic to the procedural rather than substantial aspect of tax evasion legislation. Indeed, the definition of tax evasion does not seem to have been altered by technology but rather technological innovation has simplified the modus operandi of tax evasion in certain instances. Nonetheless, constant legislative appraisals and reforms are required regarding cryptocurrency, the law of evidence, the attribution of liability to corporations for economic crimes, as well as the *mens rea* element of tax evasion offences. In terms of enforcement, it can be deduced that authorities are a step in the right direction by aiming at countering technology with its strongest opponent, technology itself. As has been identified, a competent tool for enforcement to use would be better education and awareness of technology. This chapter has thus made a cogent case for the need to consider technological innovation as an aid to effective tax evasion prevention. Thus, recommendations will be offered including a big data and blockchain technology proposal and a case will be made for why governments should apply their leverage over firms to tackle tax evasion prevention.

Big data and blockchain technology: the perfect pair?

Throughout this chapter, emerging themes have included the need to counter falsification (omissions, concealment and misrepresentation), the privacy/ information exchange dichotomy and issues with VAT and e-commerce, inter alia. In fact, one particular tool discerned by Karafiloski (2017) could tackle these challenges. This tool can be referred to as a big data and

blockchain technology hybrid, (Karafiloski, 2017). Like Connect, information gathered from institutions will be stored as big data. However, it will contain the added benefits of blockchain technology: a transaction is recorded every time a document is added to the big data system. This section seeks to identify and critically analyse its characteristics in order to make a case for why it should be implemented.

Decentralised data

First, this tool works to take on the decentralised characteristic of blockchain technology, countering privacy issues associated with centralised 'generalised' systems identified previously (Noseda, 2017). Moreover, technology called blockchain nodes enabling the moderation of access on the server will provide a secure and private way for HMRC to have bilateral and multilateral communication with taxpayers and cross-check data with third parties (Karafiloski, 2017). In fact, in the US, a white paper including the use of 'supervisory node' for on-chain regulatory surveillance was recently proposed (Adeyanju, 2020). Additionally, blockchain data is easily updated, making this tool precise and up-to-date, and thereby efficient.

Blockchain data cannot be written off and will only be accessed by concerned parties when the data is mined upon suspicion of illicit activity. To be falsified, evaders would have the virtually impossible task of deleting the whole ledger to rewrite it in their chosen way. Moreover, blockchain ledger data substantially reduces the possibility of hacking and data breaches (Rabah, 2018), which have recently occurred in the case of the cloning of the FCA register and website (Austin, Mortimer, 2020). Exploiting blockchain's non-repudiation and non-tampering properties as such would reduce the risk of identity theft enabling tax evasion, as is often the case when parties to a transaction own separate documents of the same transaction, which can easily be falsified (Xu *et al*, 2019). As a decentralised database, this method could be more applicable in an international context to counter these innumerable complex issues to combat offshore tax evasion, making it an even more effective tool in the fight against tax evasion.

A breakthrough for E-commerce

In the same way, using the blockchain ledger to record e-commerce transactions could enable better control of VAT evasion. Common methods of VAT evasion include under-reporting revenue via electronic sales suppression tools and over-reporting of deductions via false invoicing to under-report income (Amazon, 2019). However, transacting through blockchain ledgers or at least having information stored on the blockchain ledger from online platforms could counter this form of falsification. In fact, fintech tools currently being reviewed such as

mandatory HMRC-approved software and/or Electronic Point of Sale systems and fiscal tills would enable highly effective tax evasion prevention in the event that they are compatible with the big data/blockchain hybrid (HMRC, 2018). Defined as structures enabling HMRC access to transaction level data, this would remove the whole aspect of self-assessment, thereby reducing the dependence on taxpayers to be bona fide.

Accompanying effects

Such a tool could also have the effect of providing more knowledge and development to the field of cryptocurrency, potentially aiding the inception of legislation surrounding it in its midst. Moreover, it would potentially provide more insight into the shadow economy, its ghosts and moonlighters. These refer to unregistered people or people are known to the HMRC but undeclared as workers respectively (HMRC, 2020a). In fact, more extensive use of big data on both public and private ledgers, would improve transparency, as well as more trust in public administration owing to its complexity to defraud and its efficacy at detection. In turn, this would lead to greater tax morale, thereby extending its effectiveness as a tool for tax evasion prevention.

<u>An introduction to a pre-emptive strategy</u>

A concurring solution provided by Devanny et al (2018, p.89) includes the notion of regulators' investing more into next generation intelligence analysts, as a pre-emptive strategy before the economy experiences issues with a sudden 'future crisis of perceived intelligence failure'. In doing so, this would ensure detections with regards to algorithmic and human errors such as non-transparent reasoning and any cognitive bias which often precedes detection and leads to ineffective tax evasion prevention (Moses, de Koker, 2017). In its midst, this would begin to instil a more suppressive approach to tax evasion management, deemed to be most effective to prevention.

<u>Feasibility</u>

Limits to the feasibility of this proposal could include the costs involved to implement such technology. Information being decentralised, however, would make system failures avoidable and regular backups inessential, implying increased effectiveness in the fight against tax evasion.

6. Conclusion

Whilst technology is somewhat out of the legal sector's comfort zone, this study has demonstrated that now is the ideal time to take a leap of faith and implement innovative measures with the aim towards a future with less tax evasion.

Reference List

- Adeyanju, O. (2020) *Why Bitcoin Exchanges Are Building Their Own Blockchain.* Available from: https://www.forbes.com/sites/oluwaseunadeyanju/2020/04/28/why-bitcoin-exchanges-are-building-their-own-blockchain/#312611a554dd [Accessed 14th October 2020]
- Alstadsaeter, A., Johannesen, N., Zucman, G. (2019) Tax Evasion and Inequality. *American Economic Review.* 109(6), pp. 2073–2103.
- Amazon Seller Central (2019) *EU VAT Calculation Services Methodology*. Available from: https://sellercentral.amazon.co.uk/gp/help/external/help.html?itemID=202084570&ref=efph_202084570_cont_home [Accessed 14th October 2020]
- Asquith, R. [2020] The Gig and Sharing Economies: Millions of New Entrepreneurs; Billions in Lost VAT. *British Tax Review.* 1, pp.5-22.
- Austin, A., Mortimer, R. (2020) *Fraudsters Clone FCA Register and Website.* Available from: https://www.ftadviser.com/regulation/2020/07/22/fraudsters-clone-fca-register-and-website/ [Accessed 14th October 2020]
- Barberis, J., Arner, DW., Buckley, RP., eds. (2019) *The REGTECH Book: The Financial Technology Handbook for Investors, Entrepreneurs and Visionaries in Regulation*. West Sussex: Wiley.
- Beetham, F., Cape, J. (2018) Finance Act 2018 Notes: Section 38: Online Marketplaces. *British Tax Review.* 3, pp.311-323.
- Bennett, N. (2020) *When Flextime Makes For A Bad Time*. Available from: https://www.forbes.com/sites/natebennett/2020/01/09/when-flextime-makes-for-a-bad-time/#6368fce03691 [Accessed 14th October 2020]
- Bentley, D. (2020) Timeless Principles of Taxpayer Protection: How they Adapt to Digital Disruption. *eJournal of Tax Research.* 16(3), pp.679-713.
- Böhme, R., Christin, N., Edelman, B., Moore, T. (2015) Bitcoin: Economics, Technology, and Governance. *Journal of Economic Perspectives.* 29(2), pp.213-38.
- Bourton, S. (2018) Revisiting Dishonesty – The New Strict Liability Offence for Offshore Tax Evaders. In: Monaghan, C., Monaghan, N.. eds., (2018) *Financial Crime and Corporate Misconduct: A Critical Evaluation of Fraud Legislation*. London: Routledge, pp.103-117.
- Brown, SD. (2016) Cryptocurrency and Criminality: The Bitcoin Opportunity. *The Police Journal.* 89(4), pp.327-339.
- Brummer, C., Gorfine, D. (2014) *FinTech: Building a 21st-Century Regulator's Toolkit.* Available from: https://assets1c.milkeninstitute.org/assets/Publication/Viewpoint/PDF/3.14-FinTech-Reg-Toolkit-NEW.pdf [Accessed 14th October 2020]
- Dari-Mattiaccia, G., Deffains, B., Lovat, B. (2011) The Dynamics of the Legal System. *Journal of Economic Behavior & Organization.* 79(1), pp.95-107.
- de la Feria, R. (2020) Tax Fraud and Selective Law Enforcement. *Journal of Law and Society*. 47(2), pp.240-270.
- de Silva, C. (2018) *SFO Corporate Criminal Liability, AI and DPAs*. Available from: https://www.sfo.gov.uk/2018/06/21/corporate-criminal-liability-ai-and-dpas/ [Accessed 14th October 2020]
- Deloitte (2020) *RegTech Universe 2020: Take A Closer Look at Who is Orbiting in the RegTech Space.* Available from: https://www2.deloitte.com/lu/en/pages/technology/articles/regtech-companies-compliance.html [Accessed 14 October 2020]
- Department for Business, Energy & Industrial Strategy (2019) *Review of the Implementation of the PSC Register.* Available from:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/822823/review-implementation-psc-register.pdf [Accessed 4 July 2020]

- Department for Business, Energy & Industrial Strategy (2018) *Draft Registration of Overseas Entities Bill.* London: The Stationery Office. (Cm 9635)
- Devanny, J., Dover, R., Goodman, MS., Omand, D. (2018) Why the British Government Must Invest in the Next Generation of Intelligence Analysts. *The RUSI Journal.* 163(6), pp.78-89.
- Dyke, T. (2018) Ripe for Reform? Recent Developments in Search Warrants. *Judicial Review.* 23(4), pp.279-292.
- European Commission (2019) *Estimating International Tax Evasion by Individuals.* Available from: https://ec.europa.eu/taxation_customs/sites/taxation/files/2019-taxation-papers-76.pdf [Accessed 30 September 2020]
- European Parliament. (2017) *Role of Advisors and Intermediaries in the Schemes Revealed in the Panama Papers.* Available from: https://www.europarl.europa.eu/cmsdata/117285/Item_3_Study_Intermediaries_en.pdf [Accessed 14th October 2020]
- European Parliament (2016) *Tax Challenges in the Digital Economy*. Available from: https://www.europarl.europa.eu/RegData/etudes/STUD/2016/579002/IPOL_STU(2016)579002_EN.pdf [Accessed 14th October 2020]
- Gentle, S., Spinks, C., Omer, M. (2019) Proceeds of Crime Act 2002: Update 1. *Compliance Officer Bulletin.* 170, pp.1-42
- Groom, M. (2020) IR35: Far from a Fallow Year. *Tax Journal.* 1485, pp.11-13.
- Haines, A. (2017) Amazon and eBay Profiting from VAT Evaders. *International Tax Review.* Nov, pp.12-13.
- Hardouin, P. (2017) Too Big to Fail, Too Big to Jail: Restoring Liability a Lesson from HSBC Case. *Journal of Financial Crime.* 24(4), pp.513-519.
- Harrison, K., Ryder, N. (2016) *The Law Relating to Financial Crime in the United Kingdom.* 2nd ed. London: Routledge.
- Hendrikse, R. (2019) *How Deepfakes Could Become a Threat to Your Identity*. Available from: https://www.forbes.com/sites/renehendrikse/2019/12/20/how-deepfakes-could-become-a-threat-to-your-identity/#4b67320b1063 [Accessed 14th October 2020]
- Highfield, R., Evans, C., Walpole, M. (2019) The Development and Testing of a Diagnostic Tool for Assessing VAT Compliance Costs: Pilot Study Findings. *eJournal of Tax Research* [online]. 16(3), pp.620-654
- HM Revenue & Customs (2020a) *Measuring Tax Gaps 2020 Edition: Measuring Tax Gap Estimates from 2018 to 2019.* Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/907122/Measuring_tax_gaps_2020_edition.pdf [Accessed 30 September 2020]
- HM Revenue & Customs (2020b) *Cryptoasset Blockchain Analysis Tools*. Available from: https://www.contractsfinder.service.gov.uk/Notice/ec88ae4b-4f4c-4926-982a-723636cf2f82?p=1 [Accessed 14th October 2020]
- HM Revenue & Customs (2020c) *Electronic Sales Suppression: Summary of Responses.* Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/894194/Electronic_sales_suppression_Summary_of_responses.pdf [Accessed 14th October 2020]
- HM Revenue & Customs (2019a) *Guidance: HMRC's Criminal Investigation Powers and Safeguards.* Available from: https://www.gov.uk/government/publications/criminal-investigation/criminal-investigation [Accessed 14th October 2020]
- HM Revenue & Customs (2019b) *Guidance: HMRC's Criminal Investigation Policy.* Available from: https://www.gov.uk/government/publications/criminal-investigation/hmrc-criminal-investigation-policy [Accessed 14th October 2020]

- HM Revenue & Customs (2019c) *Policy Paper: Rules for Off-Payroll Working from April 2020*. Available from: https://www.gov.uk/government/publications/rules-for-off-payroll-working-from-april-2020/rules-for-off-payroll-working-from-april-2020 [Accessed 14 October 2020]
- HM Revenue & Customs (2018) *Electronic Sales Suppression: Call for Evidence*. Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/765247/Electronic_sales_suppression_-_call_for_evidence.pdf [Accessed 14th October 2020]
- HM Revenue & Customs (2017) *Tackling Tax Evasion: Government Guidance for the Corporate Offences of Failure to Prevent the Criminal Facilitation of Tax Evasion*. Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/672231/Tackling-tax-evasion-corporate-offences.pdf [Accessed 14th October 2020]
- HM Revenue & Customs (2016) *Making Connections*. Available from: https://www.tax.org.uk/system/files_force/file_uploads/151218%20Connect%20Briefing_Public%20v1.0.pdf?do [Accessed 1 October 2020]
- HM Revenue & Customs (2015) *Tax Administration: Regulations to Implement the UK's Automatic Exchange of Information Agreements*. Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/413976/TIIN_8148_tax_admin_automatic_exchange.pdf [Accessed 10 August 2019]
- HM Revenue & Customs, HM Treasury (2019) *No Safe Havens 2019: HMRC's Strategy for Offshore Tax Compliance*. Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/802253/No_safe_havens_report_2019.pdf [Accessed 10 August 2019]
- Hufnagel, S., King, C. (2020) Anti-Money Laundering Regulation and the Art Market. *Legal Studies.* 40(1), pp.131-150
- Hyde, I., Greene, M. (2020) Tax Risks in the Gig Economy: Large Business as HMRC's Policeman. *Compliance & Risk.* 9(1), pp.2-5.
- Indvik, L., Abboud, L. (2020) *Dressing Up Again? Fashion Tries to Recover from "Brutal" Crisis.* Available from: https://www.ft.com/content/89e9de1c-0213-49b8-82ba-edca04e1e910 [Accessed 1 October 2020]
- International Consortium for Investigative Journalists (2016*) Giant Leak of Offshore Financial Records Exposes Global Array of Crime and Corruption*. Available from: https://panamapapers.icij.org/20160403-panama-papers-global-overview.html [Accessed 30th September 2020]
- International Consortium for Investigative Journalists (2015) *Banking Giant HSBC Sheltered Murky Cash Linked to Dictators and Arms Dealers*. Available from: http://www.icij.org/project/swiss-leaks/banking-giant-hsbc-sheltered-murky-cash-linked-dictators-and-arms-dealers [Accessed 30th September 2020]
- Jordanoska, A. (2017) Case Management in Complex Fraud Trials: Actors and Strategies in Achieving Procedural Efficiency. *International Journal of Law in Context*. 13(3), pp.336-355.
- Karafiloski, E. (2017) *Blockchain Solutions for Big Data Challenges: A Literature Review*. Available from: https://ieeexplore.ieee.org/document/8011213 [Accessed 14th October 2020]
- Law Commission (2018) *Search Warrants: Consultation Paper No. 235*. Available from: https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2018/06/Search-Warrants-final-consultation-paper-12062018.pdf [Accessed 14th October 2020]
- Leighton-Daly, M. (2019) Identity Theft and Tax Crime: Has Technology Made It Easier to Defraud the Revenue? *eJournal of Tax Research.* 16(3), pp.578-593.
- Luttmer, EFP., Singhal, M. (2014) Tax Morale. *The Journal of Economic Perspectives*. 28(4), pp.149-68.
- Marian, O. (2013) Are Cryptocurrencies Super Tax Havens? *Michigan Law Review First Impressions.* 112(38), pp.38-48.

- Marjit, S., Seidel, A., Thum, M. (2017) Tax Evasion, Corruption and Tax Loopholes. *German Economic Review.* 18(3), pp.283-301.
- McCracken, MSK. (2002) Going, Going, Gone… Global: A Canadian Perspective on International Tax Administration Issues in the 'Exchange-of-Information Age'. *Canadian Tax Journal.* 50(6), pp.1869-1912.
- Meads, R., Jarvis, E. (2014) In Practice: Practice Points: Rules Governing Trusts. *Law Society Gazette,* 111(25), p.36.
- Milford, A. (2017) *Speech: Deferred Prosecution Agreements.* Available from: https://www.sfo.gov.uk/2017/09/05/alun-milford-on-deferred-prosecution-agreements/ [Accessed 14th October 2020]
- Ministry of Justice (2017) *Corporate Liability for Economic Crime: Call for Evidence.* London: The Stationery Office. (Cm 9370)
- Moses, LB., de Koker, L. (2017) Open Secrets: Balancing Operational Secrecy and Transparency in the Collection and Use of Data by National Security and Law Enforcement Agencies. *Melbourne University Law Review.* 41(2), pp.530-570.
- Noseda, F. (2017) Common Reporting Standard and EU Beneficial Ownership Registers: Inadequate Protection of Privacy and Data Protection. *Trusts & Trustees.* 23(4), pp. 404-409.
- OECD (2020) *Glossary of Tax Terms.* Available from: https://www.oecd.org/ctp/glossaryoftaxterms.htm [Accessed 30 September 2020]
- OECD (2019a) *AEOI: Status of Commitments*. Available from: https://www.oecd.org/tax/transparency/AEOI-commitments.pdf [Accessed 14th October 2020]
- OECD (2019b) *Tax Morale What Drives People and Businesses to Pay Tax*. Paris: OECD Publishing.
- OECD (2017) *Technology Tools to Tackle Tax Evasion and Tax Fraud.* Paris: OECD Publishing.
- OECD (2014) *Standard for Automatic Exchange of Financial Account Information in Tax Matters*. Paris: OECD Publishing.
- O'Flaherty, MC. (2019) The Rise and Rise of the Designer Resale Market. Available from: https://www.ft.com/content/a7e5d5f8-7c91-11e9-8b5c-33d0560f039c [Accessed 14th October 2020]
- OpenText (2018) *UK Serious Fraud Office Selects OpenText to Expedite Data Discovery and Investigations.* Available from: https://www.opentext.com/about/press-releases?id=27DE2D13774A4B8E82776CBEBFF19D40 [Accessed 14th October 2020]
- Ormerod, D., Laird, K. (2020) The Future of Dishonesty - Some Practical Considerations. *Archbold Review*. 6, pp.8-10.
- Ormerod, D., Laird, K., (2015) *Smith and Hogan's Criminal Law.* 14th ed. Oxford: Oxford University Press.
- Ormerod, D. (1998) Cheating the Public Revenue. *Criminal Law Review.* Sep, pp. 627-645.
- Palmer, K. (2015) *HMRC Targets Etsy, eBay and Gumtree Sellers – But When is your Hobby Taxable?* Available from: https://www.telegraph.co.uk/finance/personalfinance/household-bills/11632478/HMRC-targets-Etsy-eBay-and-Gumtree-sellers-but-when-is-your-hobby-taxable.html [Accessed 14th October 2020]
- Parker, J. (2019) *U.K. Tax Authority and Tax Fraud Investigations.* Available from: https://news.bloombergtax.com/daily-tax-report-international/insight-u-k-tax-authority-and-tax-fraud-investigations [Accessed 14th October 2020]
- Parliament. House of Commons, Committee of Public Accounts (2017a) *Tackling Online VAT Fraud and Error, Session 2017-19.* London: The Stationery Office. (HC 2017-19 312)
- Parliament. House of Commons, HM Treasury (2017b) *Autumn Budget 2017, Session 2017-19.* London: The Stationery Office. (HC 2017-19 587)
- Parliament. House of Commons, National Audit Office (2017c) *HM Revenue & Customs Investigation into Overseas Sellers Failing to Charge VAT on Online Sales, Session 2016-17.* London: The Stationery Office. (HC 2016-17 1129).

- Parliament. House of Commons, HM Treasury (2016). *Summer Budget 2015, Session 2015-16*. London: The Stationery Office (HC 2015-16 264)
- Pickhardt, M., Prinz, A. (2012) The Nature of Tax Evasion and the Shadow Economy. In Prickhardt, M., Prinz, A. eds., (2012) *Tax Evasion and the Shadow Economy.* Cheltenham: Edward Elgar, pp.3-12.
- Pijnenburg, M., Kowalczyk, W., van der Hel-van Dijk, L. (2017) A Roadmap for Analytics in Taxpayer Supervision. *The Electronic Journal of e-Government.* 15(1), pp.19-32.
- Pross, A., Kerfs, P., Hondius, P., Housden, R. (2017) Turning Tax Policy into Reality – Global Tax Transparency Goes Live. *International Tax Review.* 27(10), pp.16-21.
- Rabah, K. (2018) Convergence of AI, IoT, Big Data and Blockchain: A Review. *The Lake Institute Journal.* 1(1), pp.1-18.
- Rigney, P. (2016) *The All Seeing Eye – An HMRC Success Story?* Available from: https://www.ifa.org.uk/media/653935/Tax-HMRC-Connect-system.pdf [Accessed 14th October 2020]
- Salter, D. (2002) Some Thoughts on Fraudulent Evasion of Income Tax. *British Tax Review.* 6, pp.489-505.
- Sanghrajka, J. (2020) Degrees of Connection. *Taxation.* 186(4752), pp.8-10.
- Seddon, J., Berges, P., Stott, C., Howard, A., Paul, R., Saunders Gregor, K. (2020) *Cum/Ex Convictions- Implications for Financial Institutions in the UK*. Available from: https://www.ropesgray.com/en/newsroom/alerts/2020/03/Cum-ex-convictions-implications-for-financial-institutions-in-the-UK [Accessed 14th October 2020]
- Segal, D. (2020) *It May Be the Biggest Tax Heist Ever. And Europe Wants Justice*. Available from: https://www.nytimes.com/2020/01/23/business/cum-ex.html [Accessed 14th October 2020]
- Srivastava, A., Moffatt, N., Burkova, K., Best, T., Dayanim, B., Flickr, S. (2019) Money Laundering Update. *Compliance Officer Bulletin.* 167, pp.1-23.
- Srivastava, A., Simpson, M., Thomson, C., Tomas, J., Dennien, PM., Garfield, H., Powell, R. (2018) Financial Crime Update. *Compliance Officer Bulletin*. 157, pp.1-30.
- Tax Journal (2019) *HMRC Prosecutions against Individuals Reach 1,000s*. Available from: https://www.taxjournal.com/articles/hmrc-prosecutions-against-individuals-reach-1-000 [Accessed 14th October 2020]
- The Economist (2013) *The Rise of the Sharing Economy*. Available from: https://www.economist.com/leaders/2013/03/09/the-rise-of-the-sharing-economy [Accessed 14th October 2020]
- Turner, S., Bainbridge, J. (2018) An Anti-Money Laundering Timeline and the Relentless Regulatory Response. *Journal of Criminal Law.* 82(3), pp.215-231.
- Virgo, E. (2019) Trust Registers and Transparency: A Step Too Far? *Trust Law International.* 33(3), pp.95-112.
- Volkin, M. (2020) *Why the Gig Economy Will Drive the Future of Employment*. Available from: https://www.forbes.com/sites/forbescoachescouncil/2020/03/27/why-the-gig-economy-will-drive-the-future-of-employment/#419d87a74f52 [Accessed 14th October 2020]
- Weber, RH., Baisch, R. (2018) FinTech - Eligible Safeguards to Foster the Regulatory Framework. *Journal of International Banking Law and Regulation.* 33(10), pp.335-350
- Werle, N. (2018) Prosecuting Corporate Crime when Firms Are Too Big to Jail: Investigation, Deterrence, and Judicial Review. *The Yale Law Journal*. 128, 1366-1438.
- Xu, C., Wang, K., Li, P., Guo, S., Luo, J., Ye, B., Guo, M. (2019) Making Big Data Open in Edges: A Resource-Efficient Blockchain-Based Approach. *IEEE Transactions on Parallel and Distributed Systems*. 30(4), pp.870-882.
- Yeoh, P. (2018) Financial Secrecy Business Offshore and Onshore. *Company Lawyer.* 39(9), pp.279-285.
- Yorke, C. (2017) Dishonesty and the Failure to Prevent Evasion. *Tax Journal.* 1377, p. 16.
- Zucman, G. (2014) Taxing Across Borders: Tracking Personal Wealth and Corporate Profits. *The Journal of Economic Perspectives.* 28(4), pp.121-48.