# **Recent Developments**

Time never stands still and although coverage of Corona virus has replaced Brexit of a staple of news programmes, legal developments continue in the field of IT law with the Supreme Court delivering two significant decisions in the fields of data protection and computer crime and also an interesting High Court decision on the property status of cybercurrencies.

# Data Protection – A Matter of Life or Death?

A decade or so ago, data protection legislation was widely considered to be a peripheral and largely unwanted piece of legislation. Times have changed and the recent decision of the UK Supreme Court in the case of *Elgizouli and Secretary of State[[1]](#footnote-1)* illustrates that it can literally be a determinant of life or death.

The case had its origins in the Middle East and the activities of the, so called Islamic State (Daesh) in armed conflicts in Syria and Iraq. Numerous atrocities too place including the beheading of a number of British and United States citizens who had been captured and held hostage by Daesh. Large numbers of foreign citizens travelled to the Middle East to fight with Daesh including a group of British men (frequently referred to in the media as the “Beatles” on account of their accents) who were involved in some of the most notorious atrocities. Two of these individuals were captured by opposing forces and subsequently handed over to the United States authorities. The United States, however, proposed to initiate proceedings on charges that might result in the imposition of the death penalty and sought information from the UK under established mutual assistance procedures. In line with long-standing precedent, the UK government initially sought assurances from the US authorities that if it supplied the information, the individuals concerned would not be subjected to the death penalty. Originally it appeared that these would be forthcoming, but a new Administration under President Trump took a different line and substantial political pressure was put on the UK to transfer the information without conditions. This resulted in the then Home Secretary instructed that the data was to be sent to the United States without any assurances being sought or received. The present proceedings were instituted by the mother of one of the individuals involved and, *inter alia*, sought a declaration that the transfer of data contravened the requirements of the Data Protection Act 2018, in particular its provisions relating to the regulation of transborder data flows

The key provisions involved were contained in sections 73-66 of the Data Protection Act 2018 specifying the circumstances under which personal data might be transferred outside the European Union. This part of the statute is concerned with the processing of personal data for the purpose of law enforcement and is intended to implement Directive 2016/680 “on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data” (the “Law Enforcement Directive”). The provisions are broadly similar to those relating to more general categories of data laid down in the General Data Protection Regulation (GDPR). Under section 73 it is provided that data may be transferred to a third country only if each of 3 tests or gateways can be satisfied:

1. … the transfer is necessary for any law enforcement purpose

2. The Commission has made a finding of adequacy in respect of the third country or where appropriate safeguards can be demonstrated or where special circumstances apply

3. The party in the third country to whom the data will be disclosed is a “relevant authority”. This term is defined as being equivalent to the concept of “competent authority” used in the domestic context by the act and which identifies in Schedule 7 a wide range of investigative and prosecution authorities.

The final gateway was non-contentious in the present case with it being accepted that the US agencies to whom the data was transferred responsible for the bringing of criminal prosecutions and should be classed as relevant authorities. Attention focussed on the criterion of “necessity” and also on the nation of the safeguards and special circumstances referred to in the second gateway.

Necessity

The word “necessity” (or “necessary”) features prominently in human rights legislation, generally being used to limit the scope of exceptions to specified rights. The Data Protection Act provides for a range of situations in which personal data might be transferred outside the EU but in respect of most of these a condition of necessity will require to be satisfied. Dictionary definitions refer to notions such as “essential, obligatory, indispensable and required” and a similar approach is taken in the legal context. As was stated by Lady Hale in the Supreme Court:

In *Guriev v Community Safety Development (UK) Ltd* [2016] EWHC 643 (QB), Warby J held (in the context of restricting the subject’s right of access to his personal data) that: “The test of necessity is a strict one, requiring any interference with the subject’s rights to be proportionate to the gravity of the threat to the public interest” (para 45). The parties agree that the same test applies in this context. (at para 9)

She continued:

… it is instructive that recital (72) to the LED regards these as derogations from its requirements and as such they should be interpreted restrictively and limited to data which are “strictly necessary”. (at para 6)

The Data Protection Act provides for a balancing exercise to be performed so that prior to authorising a transfer the data controller must assess whether the “fundamental rights and freedoms of the data subject override any public interest in the transfer.”[[2]](#footnote-2) It continues to state that

 … , a transfer is necessary for a legal purpose if—

(a) it is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings) relating to any of the law enforcement purposes,

(b) it is necessary for the purpose of obtaining legal advice in relation to any of the law enforcement purposes, or

(c) it is otherwise necessary for the purposes of establishing, exercising or defending legal rights in relation to any of the law enforcement purposes.[[3]](#footnote-3)

Adequacy or Appropriate Safeguards

It was common ground that no Commission determination of adequacy existed in respect of the United States in order to justify the transfer of data. The next and related ground justifying a transfer is that “appropriate circumstances” can be demonstrated. The Data Protection Act provides that

1) A transfer of personal data to a third country or an international organisation is based on there being appropriate safeguards where—

(a) a legal instrument containing appropriate safeguards for the protection of personal data binds the intended recipient of the data, or

(b) the controller, having assessed all the circumstances surrounding transfers of that type of personal data to the third country or international organisation, concludes that appropriate safeguards exist to protect the data.

The Act continues to require that:

(3) Where a transfer of data takes place in reliance on subsection (1)—

(a) the transfer must be documented,

(b) the documentation must be provided to the Commissioner on request, and

(c) the documentation must include, in particular—

(i) the date and time of the transfer,

(ii) the name of and any other pertinent information about the recipient,

(iii) the justification for the transfer, and

(iv) a description of the personal data transferred.

Evidencing the fact that in some quarters the Data Protection Act continues to be regarded as a trivial matter, the Court was critical of the manner in which the then Home Secretary, and also the Divisional Court which heard the case at first instance, had approached the task of determining whether the data should be transferred to the United States. As was noted in the judgement of Lady Hale:

The short point is that, insofar as the information provided, or to be provided, to the US authorities consisted of personal data (which much of it did) the processing of such data by the Secretary of State as data controller required a conscious, contemporaneous consideration of whether the criteria for such processing were met. “Substantial compliance” with those criteria, as found by the Divisional Court, is not enough. It is not in dispute that the Secretary of State, when making the decision in question, did not address his mind to the 2018 Act at all. (at para 1)

Lord Kerr made a similar point:

I consider that the requirement that the data be limited to that which is strictly necessary behoves the data controller to make an assessment of what, in the context of the DPA, is strictly necessary and, since it is accepted that the Home Secretary did not have regard to his duties as data controller, the special circumstances gateway was not available. Moreover, it is not enough to say that the data protection provisions were substantially met, where direct, personal evaluation was required. (at para 158)

Beyond procedural aspects, the Directive’s recitals refer to more substantive aspects

“Transfers not based on such an adequacy decision should be allowed only where appropriate safeguards have been provided in a legally binding instrument which ensures the protection of personal data or where the controller has assessed all the circumstances surrounding the data transfer and, on the basis of that assessment, considers that appropriate safeguards with regard to the protection of personal data exist … In addition, the controller should take into account that the personal data will not be used to request, hand down or execute a death penalty or any form of cruel and inhuman treatment …”

The terms of the Recitals were criticised

“… if this recital were intended to be a ‘red-line prohibition’ it (a) would be expressed clearly as such, (b) would be expressed in imperative terms (‘must’ rather than ‘should’ and not merely ‘take into account’), and (c) would be in an article rather than a recital.” (at para 182)

The Supreme Court disagreed:

It is true that recital (71) is no more than an interpretative aid, and that its wording could be clearer. However, the words “will not be used” seem to leave little room for discretion. The expectation is that the appropriate safeguards will be designed to achieve that objective. That is also consistent with the government’s long-standing policy of seeking full death penalty assurances in all cases. Given that in this case the information was transferred without any safeguards at all, I am unable to see how (if the question had been considered) the Secretary of State could have regarded this condition as satisfied. The Divisional Court was wrong in my view to find otherwise. (at para 220)

Special Circumstances

The final gateway through which data could lawfully have been transferred would see the existence of, so called, “special circumstances. These are defined in section 76(1) of the Act as applying in circumstances where the transfer is necessary in order:

(a) to protect the vital interests of the data subject or another person,

(b) to safeguard the legitimate interests of the data subject,

(c) for the prevention of an immediate and serious threat to the public security of a member state or a third country,

(d) in individual cases for any of the law enforcement purposes, or

(e) in individual cases for a legal purpose.”

The Divisional Court held that the transfer of data could be justified on the ground of special circumstances. The Supreme Court held unanimously that this was incorrect. The grounds upon which counsel for the Secretary of State relied upon are paragraphs (d) and (e). The term “legal purpose” referred to in paragraph (e) is defined as “any legal proceedings (including prospective legal proceedings) …”[[4]](#footnote-4) The Act continues to provide that:

… subsection (1)(d) and (e) do not apply if the controller determines that fundamental rights and freedoms of the data subject override the public interest in the transfer.[[5]](#footnote-5)

Once again, the spectre of necessity loomed over the decision-making process. As was stated by Lord Carnwath:

It is apparent that the decision was based on political expediency, rather than strict necessity under the statutory criteria. There was no consideration as to whether transfer of “personal data” as such was required. There was also a notable lack of any assurance, if the information were made available, as to the prospects of a prosecution in fact taking place in the US. Given that there was insufficient evidence to prosecute in the UK, it is not clear why the legal position was thought to be any different in the US. So long as the prospects of any prosecution was uncertain, it would seem premature to say that any particular information was “strictly necessary” for that purpose. Of course, if there were no prosecution, concerns about the risk of the death penalty would fall away, but that in itself could not affect the need for the transfer to be justified under the statutory criteria. (at para 227)

The test of “necessity” can be relevant across a range of contexts. It could be argued that the present transfers were necessary for political reasons. The judgments in the Supreme Court indicate, however, that necessity has to be judged solely by reference to legal factors.

Could there be any acceptable justifications for transfer?

The key basis upon which the Supreme Court held that there had been a breach of the Data Protection Act was essentially the failure on the part of the Secretary of State to follow due process. It is perhaps not surprising that, given the clear terms of the Data Protection Act and the clear (although perhaps poorly worded) provisions of the Law Enforcement Directive, this was the conclusion reached. The conclusion that the process followed by the Secretary of State was fundamentally flawed meant that relatively little consideration was given to more substantive issues. There are, however, some significant indications in the judgments of Lady Hale and Lord Carnwath that should be noted. Lady Hale commented that:

The most fundamental of the rights protected by the European Convention is the right to life. This is an absolute right, not qualified by the possibility of restrictions or interferences which are “necessary in a democratic society”. Article 2.1 prohibits the state from taking anyone’s life intentionally: the former exception for the death penalty when provided by law has gone following the Sixth and Thirteenth Protocols to the European Convention …

… Collectively, these provisions point towards an interpretation of section 76(2) which would not allow the transfer of personal data to facilitate a prosecution which could result in the death penalty; but which would allow such a transfer if it was urgently necessary to save life or prevent an imminent crime. Had it been necessary, I would have been prepared so to hold. (at paras 9-10)

These sentiments obtained a measure of support from Lord Carnwath

Although I would have welcomed fuller argument on the point, I see the force of her comments. At the least, failure to consider this point is a further reason for holding that the decision cannot stand. (at para 228)

On this basis, a transfer of personal data would never be permitted where this might result in the imposition of the death penalty.

Cyber-currency as Property?

*AA v 1) Persons Unknown Who Demanded Bitcoin on 10th And 11th October 2019 (2) Persons Unknown Who Own/Control Specified Bitcoin (3) Ifinex Trading as Bitfinex (4) Bfxww Inc Trading as Bitfinex*

The claimant, AA, was an insurance company who had provided cover to a client whose electronic data had been encrypted by hackers who demanded and received a ransom payment of around $1,000,000 in Bitcoins in order to be provided with the decryption programs enabling their data to be restored.

Following payment (and successful recovery of the affected data) the claimant insurer sought to track down the individuals involved. A specialist company was contracted which was able to trace the ransom payment to a crypto currency exchange operating under the name of “Bitfinex” – the third and fourth defendants in the present case (the first 2, unnamed, defendants were the unknown perpetrators of the crime). A crypto-currency exchange, as the name might suggest, facilitates the exchange of Bitcoins or other systems of crypto-currency into realisable fiat currencies. Bitfinex is a cryptocurrency exchange owned and operated by iFinex. Its headquarters are in Hong Kong and the company’s registered office is in the British Virgin Islands – a territory which had been placed on the EUs list of countries considered to be tax havens.

The claimant sought an order from the High Court requiring the operators of the currency exchange to disclose such information as they might possess facilitating the claimant’s task of identifying and seeking recovery of the ransom from the presently unknown perpetrators. It also, and the main focus of this stage of the proceedings, sought a proprietary injunction declaring its entitlement to ownership of the Bitcoins associated with the ransom payment. The issue that arose here was that such an injunction can be awarded only in respect of interests in property and the court had to determine whether Bitcoin (and other crypto currencies) should be classed as a form of property. Further factors complicating the proceedings lay in the international nature of the Bitcoin exchange’s operations and concerning the question whether proceedings in the case, at least at the present stage, should be conducted in private or in open court?

In this case, and it would appear likely that the same factors would apply in similar proceedings, it was held that the proceedings should be conducted in private. The judge ruled that: “… publicity would defeat the object of the hearing. It would potentially tip off the persons unknown to enable them to dissipate the Bitcoins; secondly, there would be the risk of further cyber or revenge attacks on both the Insurer and the Insured Customer by persons unknown; there would be a risk of copycat attacks on the Insurer and/or the Insured Customer and I am satisfied that in all the circumstances it is necessary to sit in private so as to secure the proper administration of justice.”[[6]](#footnote-6)

 The case, it was held, was analogous to proceedings involving blackmail and although the report of the judgment was published – albeit with the redaction of some confidential data and with the identity of the claimant remaining concealed.

The critical question before the court was whether cryptocurrency could be classed as “property” in English law? The notion of “property is very much a cornerstone of the legal system but is a concept which challenges precise definition. It may refer to a thing itself and also to a legal relationship between a person and a thing. Property is divided into a number of categories with a basic distinction being between “choses (or things) in possession” and “choses in action”. The term “choses in Possession” relates effectively to objects where the value lies primarily in the physical elements contained therein. A motor car might be an example of a chose in possession. “Choses in action” refers to a right in respect of property that can only be enforced by means of a legal action. An example might be a debt or a claim to damages for breach of contract. Such claims can be pursued only by means of legal proceedings.

 The term “property” features in a wide range of statutes. Relevant to the present discussion the Theft Act 1968 defines the eponymous offence and provides in section 4 that:

1. “Property” includes money and all other property, real or personal, including things in action and other intangible property.

 The concept of “money” is not defined further in English Law. Some assistance can be found in the concept of legal tender although as described by the Bank of England this is of theoretical rather than practical significance. There is no doubt that the theft of a foreign currency bank note, such as a US Dollar, will be susceptible of prosecution in the UK and it may be that the term money is to be interpreted in the sense of a currency issued or recognised by a Central Bank. The essence of crypto-assets, of course, is that they are not issued by a central authority. Can they still be classed as property? In respect of these it was suggested in the present case that: “… they are virtual, they are not tangible, they cannot be possessed.”[[7]](#footnote-7)

The judge continued: “Prima facie there is a difficulty in treating Bitcoins and other crypto currencies as a form of property: they are neither chose in possession nor are they chose in action. They are not choses in possession because they are virtual, they are not tangible, they cannot be possessed. They are not choses in action because they do not embody any right capable of being enforced by action. That produces a difficulty because English law traditionally views property as being of only two kinds, choses (things) in possession and choses in action. In *Colonial Bank v Whinney* [1885] 30 Ch.D 261 Fry LJ said:

“All personal things are either in possession or action. The law knows no *tertium quid* (third way) between the two.”[[8]](#footnote-8)

 The *Colonial Bank* case arose out of a situation in which a party had obtained a loan from a bank offering share certificates as security for the lean. The debtor was subsequently made bankrupt and a dispute arose between the trustee in Bankruptcy – who was responsible for realising the debtor’s assets and distributing them to creditors - and the back as to the rights in the shares deposited as security. At the time of the case, the relevant Statute was the Bankruptcy Act 1883. Section 50(3) of the Act provided that:

 Where any part of the property of the bankrupt consists of things in action, such things shall be deemed to have been duly assigned to the trustee.

On this basis, the Bank’s claim to the shares was rejected by Lord Justice Fry who was in the minority in the Court of Appeal but whose decision and reasoning was supported in a further appeal to the House of Lords. The case has been cited subsequently as authority for the proposition that there is a dichotomy between choses in possession and choses in action and that, in the eyes of the law, if something is not a chose in possession or action it cannot be classed as property in its legal sense In the present case, this approach was considered to represent an oversimplification of a complex issue:

“… on a more detailed analysis I consider that it is fallacious to proceed on the basis that the English law of property recognises no forms of property other than choses in possession and choses in action.”[[9]](#footnote-9)

 The question in *Colonial Bank*, it was stated,was limited to whether the shares were things in action for the purpose of the particular statute, not whether they were property in a more general sense.

 Shortly before the judgement a “Legal statement on cryptoassets and smart contracts”[[10]](#footnote-10) was published by the UK Jurisdictional Task Force (“UKJT”). Established under the auspices of the LawTech Delivery Panel, which is described as “an industry-led, government-backed initiative, established to support the transformation of the UK legal sector through tech”[[11]](#footnote-11), the Jurisdictional Task aims to” ensure that English law and the jurisdiction of England and Wales together provide a robust foundation for the development of DLT, smart contracts, and associated technologies”. The Legal Statement on Cryptoassets published in November 2019 marks the first fruit of its labours[[12]](#footnote-12). It contains a detailed analysis of the decision in Colonial Bank and other authorities and concluded:

 A categorisation of the elements required for property to be legally recognised as such is found in *National Provincial Bank v Ainsworth[[13]](#footnote-13)*. In this case it was ruled that before a right or an interest could be classed as property, it must be

 “*…definable, identifiable by third parties*, capable in its nature of assumption by third parties, and have some degree of *permanence or stability*. Other authorities have referred to the qualities of *certainty, exclusivity, control* and *assignability*.”[[14]](#footnote-14)

After considering the authorities, the task force statement concluded:

 “(a) crypto-assets have all of the indicia of property;

(b) the novel or distinctive features possessed by some cryptoassets—intangibility, cryptographic authentication, use of a distributed transaction ledger, decentralisation, rule by consensus—do not disqualify them from being property;

(c) nor are crypto-assets disqualified from being property as pure information, or because they might not be classifiable either as things in possession or as things in action”[[15]](#footnote-15)

 The conclusion that was expressed was that a crypto-asset might not be a thing in action on a narrow definition of that term, but that it should be treated as property. This view was endorsed by the judge who whilst recognising that the task force statement had no legal authority concluded.

 “Essentially, and for the reasons identified in that legal statement, I consider that a crypto asset such as Bitcoin are property.”[[16]](#footnote-16)

The issue then arose as to the nature of the remedies that might be available to the claimant and as to the procedures that should be followed. The prime desire on the part of the claimants was obviously to retrieve the bitcoins that had been unlawfully taken from them. This could involve a lengthy legal process and the first order that was sought and obtained was to require the Bitcoin exchange (the third and fourth defendants in the case) to take steps to ensure that the coins were not moved outside their control. The exchange would also have information facilitating the identification of the alleged criminals (the first and second defendants) and it was required to disclose this. This much of the judgment is fairly routine. A complicating factor was that the Bitcoin exchange (and the contested bitcoins) was located outside the UK. Did the English courts have jurisdiction to hear the case? The answer was a fairly unambiguous “yes”.

It is a basic tenet of the law that a defendant should be made aware of the nature and extent of any claims that may be made against it in legal proceedings. Historically, this involved the personal delivery of a written notice of claim but more modern methods such as service by email are also permitted where the court considers that the circumstances warrant this. In the present case it was noted that:

“So far as the third and fourth defendants are concerned, communication to date has been by email and what is sought is service by email to three email addresses, two previously used and one more recently used. I need to give more careful consideration in the case of the third and fourth defendants because they have recently communicated saying that they require to be served in the BVI and therefore the cooperative approach which they had been indicating they were going to adopt, that they could be served by email which also appears to be their normal method of service, i.e. they accept service by email (which may reflect the fact that they are indeed a technology company), they have now indicated they want to be served in person in the BVI. That does cause me some concern because they have also said in the same breath that they will cooperate with the court and any court order the court may make.”[[17]](#footnote-17)

It would appear that the judge was somewhat suspicious of the motives of the operators of the Bitcoin exchange.. It was held that service of notice to identify the main defendants could validly be made by email directed to addresses previously used by the defendants in communications related to the case. Insofar as the first and second defendants (potentially the same people) service was to be directed to the email addresses used to send the original ransom demands.

Vicarious liability and computer misuse

Another relevant Supreme Court decision is that of *WM Morrison Supermarkets plc v Various Claimants*[[18]](#footnote-18)*.* This concerned the extent of the liability of a company for actions of an employee that resulted in the wrongful disclosure of personal data about other employees in breach of the Computer Misuse and Data Protection Acts. The incident occurred seven years ago in 2013. An employee, Andrew Skelton, had been disciplined for what were described as relatively minor incidents of misconduct but subsequently harboured a grudge against his employers. Revenge took the form of his obtaining (in the course of his contracted duties) a copy of details of the names of all employees, their home addresses and a range of financial data including details of bank accounts and posting these to a file-sharing web site. He then sent CDs containing the data anonymously to three UK newspapers purporting to be a concerned member of the public who had found the data on the file-sharing website. The newspapers did not publish the data but rather contacted Morrisons who launched investigations into the conduct. The cost of these and the adoption of identity was estimated at £2.6 million. Criminal prosecution followed and the employee was sentenced to a term of 8 year’s imprisonment on charges of fraud and breach of the Computer Misuse and Data Protection Acts.

The present proceedings were brought in the name of almost 10,000 employees of Morrison following the making of a group litigation order by the High Court. They sought compensation from Morrison for the damage and distress caused to them by the misuse of their personal data. Three key issues were raised, whether Morrison should be held vicariously liable at Common Law for their employee’s conduct and, if so, whether the Data Protection Act (in this case the Act of 1998) excluded the imposition of vicarious liability for statutory torts committed by an employee data controller and, finally, whether the Data Protection Act excluded the imposition of vicarious liability for misuse of private information and breach of confidence?

The issue of vicarious liability was critical to the case. This is concerned with the liability of employers for the actions of their employees and is likely to assume greater significance as we move into the, so called, “gig economy” where the distinction between contracts of employment and contracts for services can be blurred. The issue that typically arises is whether the actions of an individual are sufficiently connected with their employment duties as to make it equitable to hold the employer responsible in the event that another party suffers loss. In the present case, potentially thousands of Morrison’s employees could claim to have suffered. There would be no doubt that the individual concerned would be potentially liable but extremely unlikely that that person would have sufficient financial resources to satisfy and award of compensation. It is general practice in litigation to seek to impose liability on the party with the deepest pockets. The key factor in determining whether an employer should be held vicariously liable for the acts of employees looks at how closely the act complained of relates to the exercise, albeit in an improper manner, of the employees work related duties. An employer would not be liable if the employee was, in the oft used term “on a frolic of his own”. After surveying a range of authorities, the Supreme Court held that this was not the case. One significant factor was that the conduct had been intended to damage the employer. In a sense the losses incurred by other employees were ancillary to this. The court stated

In the present case, it is abundantly clear that Skelton was not engaged in furthering his employer’s business when he committed the wrongdoing in question. On the contrary, he was pursuing a personal vendetta, seeking vengeance for the disciplinary proceedings some months earlier. In those circumstances… Skelton’s wrongful conduct was not so closely connected with acts which he was authorised to do that, for the purposes of Morrisons’ liability to third parties, it can fairly and properly be regarded as done by him while acting in the ordinary course of his employment. (para 47)

There is no doubt that the injured employees would have been able to take action against the wrongdoer. The Court indicated that he was to be considered a data controller in his own right and the Data Protection Act gives a right to claim compensation for any damage and distress caused by a breach of the data protection principles and there seems little doubt that this will have occurred. Morrison would also, of course, be classed as a data controller and it would appear that they would now be jointly and severally liable under the provisions of Article 82(4) of the GDPR. Under the 1998 Act they might incur liability in their own right for breach of the seventh data protection principle requiring the taking of “(a)ppropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.” Although the point was not discussed in detail before the Supreme Court, it is questionable whether Morrison had been in breach of the security principle? The transfer of the data to the employee was a normal element of business activity and within his normal employment remit. The Court did hold that am employer could potentially be vicariously liability for data protection breaches occurring as a result of the employee’s conduct. In the present case of course, this determination was of little relevance as the court had already determined that the employer was not vicariously liable for the particular acts in question.

1. [2020] UKSC 10. [↑](#footnote-ref-1)
2. S 76(2). [↑](#footnote-ref-2)
3. S 76(4). [↑](#footnote-ref-3)
4. S 76(4). [↑](#footnote-ref-4)
5. S 76(2) [↑](#footnote-ref-5)
6. *AA v iFINEX*, [2019] EWHC 3556 (Comm), para. 30. [↑](#footnote-ref-6)
7. *AA v iFINEX*, [2019] EWHC 3556 (Comm), para. 55. [↑](#footnote-ref-7)
8. *AA v iFINEX*, [2019] EWHC 3556 (Comm), para. 55. [↑](#footnote-ref-8)
9. *AA v iFINEX*, [2019] EWHC 3556 (Comm), para. 58. [↑](#footnote-ref-9)
10. UK Jurisdiction Taskforce, “Legal statement on cryptoassets and smart contracts”, November 2019 – available at: <https://35z8e83m1ih83drye280o9d1-wpengine.netdna-ssl.com/wp-content/uploads/2019/11/6.6056_JO_Cryptocurrencies_Statement_FINAL_WEB_111119-1.pdf> [↑](#footnote-ref-10)
11. <https://technation.io/about-us/lawtech-panel/> [↑](#footnote-ref-11)
12. Available from <https://technation.io/about-us/lawtech-panel/> [↑](#footnote-ref-12)
13. [1965] AC 1175. [↑](#footnote-ref-13)
14. Fairstar Heavy Transport NV v Adkins [2013] EWCA Civ 886. [↑](#footnote-ref-14)
15. UK Jurisdiction Taskforce, “Legal statement on cryptoassets and smart contracts”, November 2019, para. 15. [↑](#footnote-ref-15)
16. *AA v iFINEX*, [2019] EWHC 3556 (Comm), para. 59. [↑](#footnote-ref-16)
17. *AA v iFINEX*, [2019] EWHC 3556 (Comm), para. 76. [↑](#footnote-ref-17)
18. [2020] UKSC 12. [↑](#footnote-ref-18)