CHAPTER 4

Big Data: Tackling Illicit Financial Flows

Tatiana Tropina

Tatiana Tropina

Senior Researcher, Max Planck Institute for Foreign and International Criminal Law

The relatively new phenomenon of big data has rapidly become both a promise and a challenge. Big data solutions are praised by some as technologies that will change the world, criticized by others as threats to privacy, acclaimed to be a silver bullet to myriad issues, called a "buzzword tsunami," and used as a source of inspiration for utopian and dystopian scenarios; big data has quickly become central to many policy debates. Governments, law enforcement agencies, and the private sector are currently trying to grasp the benefits of the huge amounts of data generated and processed daily and exploring how big data can help them perform better in different areas—from healthcare to preventive policing and from targeted advertising to research and innovation, to name but a few. Meanwhile, criminals strive to use big data to their advantage as well.

There is still no agreed-upon definition of big data, though many define it as the rapidly increasing production, storage, and transfer of large amounts of data available from different sources, along with the algorithms and tools needed to process them. However, though its definition is still being debated, big data is already a reality. Despite ongoing debates around the use of big data tools for preventing and controlling crime, there is no question "if" these tools will be employed: the questions are only "how" and "when." There is also little doubt that, once implemented properly, big data analytics can be revolutionary in tackling illicit financial flows.

This chapter explores both how big data is used by criminals to create illicit profits and how law enforcement and other institutions can use big data to help tackle this problem. It begins with a brief explanation of the concept of illicit financial flows and examination of how digital technologies are changing the face of online and offline profit-driven crime. It also investigates the promises and challenges of using big data to stop illicit financial flows and discusses the balance between law and technology required to address the problem of illegally acquired money. Finally, recommendations highlight the need for long-term approaches to combat the problem of crime, wherein big data and other technological solutions should be made part of comprehensive strategies.

Digital Technologies and Illicit Financial Flows: State of Play and Possible Developments in the Era of Big Data

In the past few years, use of the term “illicit financial flows” has grown; these illegal flows are now a crosscutting issue on the agenda of governments and international organizations such as the World Bank and Organisation for Economic Co-operation and Development (OECD), amongst others. Despite a lack of consensus regarding the extent to which this term covers grey areas and practices such as tax avoidance, the general understanding is that it refers to money “illegally earned, transferred or used.”[168] The notion of illicit financial flows aims to connect seemingly disparate illegal activities under a single umbrella to tackle the whole lifecycle of illicit finance—from earning to utilization—and provide a holistic picture of the issue. The umbrella approach makes even more sense in the digital age, where technology has increasingly become a common enabler. It also makes it possible to adopt harmonized frameworks to trace illegal money, to share best practices between regulatory domains, and, ultimately, to connect previously fragmented efforts.

The legal and technical solutions for tracing crime in a digital environment have never been perfect, and in an age of exponentially increasing data, finding solutions is now akin to finding the proverbial needle in a growing haystack of data. However, big data also makes it easier to trace criminal activity.

Illicit Profits: How Digital Technologies Are Changing the Face of Crime

As information and communications networks have changed the way of doing business and the manner of social interactions, they have also been employed by criminals to both facilitate traditional criminal activities and enable new types of crimes.

Box 4.1. Underground Economy of Cybercrime: Automation and Botnets

Automation plays a vital role in the functioning of the underground economy: without it criminals would have to manually target individual victims and computer systems, thus making attacks and crimes too costly and time consuming. The core of automation and the backbone of the underground economy are the botnets, i.e., networks of compromised computers that can be remotely controlled by the perpetrators and used as “zombies” to launch large-scale denial-of-service attacks on computer systems, disseminate malware, and look for system vulnerabilities. Trading botnets is a very profitable activity in the “crime as service” business model, which is based on offering services, such as hacking and carding, and tools to commit cybercrime for sale or rent. Botnets are offered at a low cost relative to profit due to the high volume of “customers” and overall turnover: distributed denial-of-service attacks can be purchased for $10 to $1,000 per day.[169]

The Digital Underground Economy

Cybercrime, which in the last decade has transformed into a complex and thriving digital underground economy, is one of the most direct links between digital technologies and illicit financial flows. This economy is based on the monetary value of data as an illegal commodity,[170] which is moved across national borders and traded in underground online marketplaces.[171]

Technological developments are transforming both the legitimate and illicit economies, in part by decentralizing operations as value chains are being replaced with value networks. The patterns of doing business in criminal ecosystems bear many similarities to legitimate business-to-business models regarding decentralization, product placement, outsourcing, subcontracting, and networking. And, like legitimate businesses, those in the criminal economy strive to profit from the development of new business models based on the use of information, communications technologies,

[168] United Nations Economic Commission for Africa, Report of the High Level Panel on Illicit Financial Flows from Africa, 2015, http://www.uneca.org/sites/default/files/PublicationFiles/iff_main_report_26feb_en.pdf; see also “Illicit Financial Flows (IFFs),” World Bank, 2015, http://www.worldbank.org/en/topic/financialmarketintegrity/brief/illicit-financial-flows-iffs.

[169] Europol, Threat Assessment: Internet Facilitated Organized Crime, The Internet Organised Crime Threat Assessment, File No.: 2530–264, The Hague, January 7, 2011, https://www.europol.europa.eu/sites/default/files/publications/iocta.pdf; see also Candid Wueest, “Underground Black Market: Thriving Trade in Stolen Data, Malware, and Attack Services,” Symantec Official Blog, November 20, 2015, http://www.symantec.com/connect/blogs/underground-black-market-thriving-trade-stolen-data-malware-and-attack-services

[170] For example, according to SecureWorks, in 2015-2016 the price for stolen credit card credentials varied from $4–$80 per item, the price for stolen online payment account credentials varied from $20 to $149 per item depending on the account balance, and the full packages of identity information were traded for $15–$65. See Dell, SecureWorks, Underground Hacker Markets, Annual Report – April 2016, http://online.wsj.com/public/resources/documents/secureworks_hacker_annualreport.pdf.

[171] Hanno Fallmann, Gilbert Wondracek, and Christian Platzer, “Covertly Probing Underground Economy Marketplaces,” Vienna University of Technology Secure Systems Lab, 2010, http://www.iseclab.org/papers/dimva2010_underground.pdf; Europol, The Internet Organized Crime Threat Assessment (iOCTA), 2014, https://www.eurssopol.europa.eu/content/internet-organized-crime-threat-assesment-iocta.

and analysis of digital data. These new models allow money stolen through cybercrime to generate illicit revenues, from the supply of the tools to the commission of the crimes. Highly sophisticated criminal-to-criminal services offer "crime as service" tools, including training tutorials, while making them available for "customer" demand at relatively low prices compared with the potential illicit profits.[172]

Information Technology as a New Tool for 'Traditional' Organized Crime

Criminal organizations carrying out "traditional" illegal activities use digital tools for planning and coordination, communications, networking, and trading illegal goods, including arms, drugs, and counterfeit documents. The Internet merges these activities with those related to cybercrime—such as the trade in botnets and tools to commit digital crimes and trade in stolen personal data—and outsources the commission of digital crimes. These two trends drive the creation of online criminal hubs—hidden online marketplaces—where the trade of traditional illegal goods and services coexists in the "darknet" with the supply of tools to commit cybercrimes.

A trend that is distinct from using the Internet to facilitate the trade of illegal goods, and much more worrisome, is the attempt by traditional organized crime groups to employ the skills of highly qualified cybercriminals to carry out the sophisticated manipulation of computer systems to facilitate illegal operations. One of the first studied cases of such synergy was discovered in June 2013, when law enforcement agencies detected a Netherlands-based drug smuggling ring that collaborated with hackers to penetrate the systems controlling the movement and location of shipping containers and—as a result of data manipulation—was able to collect cargos with drugs before the legitimate carrier was able to get them.[173]

Terrorist Financing

The Internet is a well-known vehicle for terrorist financing. Terrorist organizations use digital tools and communications technologies to solicit donations and conduct e-commerce schemes for selling books and promotional material to supporters. For example, a group of Islamic State of Iraq and al-Sham militants from Russia has used the very popular digital wallet QIWI to collect money online.[174]

A growing trend concerns the use of digital currencies for terrorist financing: their relative anonymity, ease of use, accessibility, and the fact that they are decentralized and mostly unregulated make them attractive means of carrying out fundraising campaigns. Some of the anti-money laundering bodies—both nationally and internationally—are discussing potential regulatory responses to the possible use of virtual currencies by terrorists. For example, the Financial Crimes Enforcement Network (FinCEN), an agency of the US Treasury Department, is considering establishing a "meaningful regulatory framework for virtual currencies that intersect with the U.S. financial system."[175] In addition, the intergovernmental Financial Action Task Force monitors emerging regulatory issues arising from terrorist financing risks associated with virtual currencies.[176]

Meanwhile, there have already been cases of terrorist organization websites requesting donations via bitcoin.[177] Social media and crowdfunding—whether being used under false pretensions or not—have also emerged as valuable fundraising tools for terrorists.[178] Terrorist organizations and radicalized individuals can also use peer-to-peer lending.[179] Since many of these opportunities use payment methods that exist outside of regulatory oversight and anti-terrorist financing compliance procedures, there is a risk that terrorist networks can use

[172] Yuval Ben-Itzhak, "The Cybercrime 2.0 Evolution," ISSA Journal, June 2008, http://professor.unisinos.br/llemes/Aula01/CybercrimeEvolution; Tatiana Tropina, "Organized Crime in Cyberspace" in Heinrich-Böll-Stiftung and Regine Schönenberg (eds.), Transnational Organized Crime: Analyses of a Global Challenge to Democracy, Bielefeld, Transcript Verlag, 2013, 47-60.

[173] Europol, iOCTA.

[174] Joanna Paraszczuk, "IS Militants Use Popular Russian Web Payment System to Raise Cash," Radio Free Europe, May, 17, 2015, http://www.rferl.org/a/islamic-state-funding-russian-web-payments-qiwi/27021379.html.

[175] FinCEN, *Statement of Jennifer Shasky Calvery, Director, Financial Crimes Enforcement Network, United States Department of the Treasury,* November 19, 2013, https://www.fincen.gov/news/testimony/statement-jennifer-shasky-calvery-director-financial-crimes-enforcement-network.

[176] Financial Action Task Force (FATF), *Guidance for a Risk-Based Approach: Virtual Currencies*, 2015, http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf.

[177] FATF, Emerging Terrorist Financing Risks, 2015, http://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf, 36.

[178] Sam Rubenfeld, "Foreign Terror-Fighters Fundraise on Social Media, Crowdfunding Sites," Wall Street Journal, October 21, 2015, http://blogs.wsj.com/riskandcompliance/2015/10/21/foreign-terror-fighters-fundraise-on-social-media-crowdfunding-sites/; FATF, Emerging Terrorist Financing Risks, 31-32.

[179] Such concerns were especially raised after it became known that Syed Rizwan Farook, one of the two shooters responsible for the terrorist attack in San Bernardino, California, on December 2, 2015, was able to get a loan of $28,500 through an online peer-to-peer lending website (see, e.g., Darrell Delamaide "Loan to Terror Couple Challenges Regulators," USA Today, December 15, 2015, http://www.usatoday.com/story/money/2015/12/15/shooting-terrorism-online-loans-san-bernardino/77358520/).

virtually any such payment and fundraising tool to their benefit.

Box 4.2. Use of Bitcoin for Terrorist Financing: Ibn Taymiyya Media Center

The case of the Ibn Taymiyya Media Center (ITMC)—an online jihadist propaganda unit located in the Gaza Strip—using bitcoin for fundraising was brought by Yaya J. Fanusie, a former counterterrorism analyst for the US Central Intelligence Agency. According to Fanusie, the ITMC used social media tools to carry out the fundraising campaign in bitcoin. This was the first known case of the terrorist group publicly seeking donations in digital currency. The terrorist unit posted the information on Twitter with QR (Quick Response) codes that were linked to a bitcoin address, which received two bitcoin donations in July 2016.[180]

Tax Fraud, Tax Evasion, and Information Technologies: The Challenges of the Digital Economy

While it is hard to assume that the use of global communications networks has no effect on tax evasion, it is unknown whether there are any specific digital tools employed in this area that help carry out large-scale corporate tax evasion. Undoubtedly, the digital economy and borderless Internet, while enabling operations worldwide, create loopholes in taxation. The possibility that tax bases are becoming severely eroded in the digital economy has prompted international organizations to place this issue on their agendas; the OECD, for example, is currently developing action plans to address the problems associated with taxation in the digital era.[181]

There is, however, a growing synergy between identity-theft cybercrimes and tax fraud. Stolen identities can be used to file tax returns: such schemes involve reporting inflated amounts of income and taxes, and, therefore, claiming inflated tax refunds. Criminals can further seek to transfer these tax refunds to prepaid debit cards.[182]

Use of Information Technologies in Illegal Money Transfers and Integration

Digital tools have significantly transformed many components of illicit financial flows, including the transfer and integration of ill-gotten gains. All stages of money laundering—placement, layering, and integration[183]—are affected by the myriad ways online transactions can be used to distance any type of illicit funds from the source of illegal profit.

Technology does not care about the source of illegal income. The same tools and digital technologies can be used to transfer illicit money of any origin, including from corruption, embezzlement, organized crime, tax evasion, and many other activities. The only difference between online and offline criminal activities for money transfers is that the profits gained from digital crime already exist in the digital environment, so money laundering's risky placement stage can be avoided.[184] The same is true for the illegal trade of goods online in digital currencies: the money is "pre-laundered" because it is placed in mostly unregulated financial institutions.[185]

The countless opportunities for digital transactions via various electronic payment intermediaries—such as transfers from one intermediary to another, peer-to-peer transactions, and transfers to and from the traditional banking system—are making the ecosystem extremely complex[186] and creating obstacles in the identification of suspicious transactions.[187] Many electronic payment intermediaries are less regulated than traditional financial institutions or not regulated at all.[188] Thus, compliance with anti-money laundering laws and the identification of suspicious transactions are left to the unregulated payment intermediary, many of which lack the incentive to detect suspicious

[180] Yaya Fanusie, "The New Frontier in Terror Fundraising: Bitcoin," The Cipher Brief, August 24, 2016, https://www.thecipherbrief.com/column/private-sector/new-frontier-terror-fundraising-bitcoin-1089.

[181] OECD, Addressing the Tax Challenges of the Digital Economy, OECD/G20 Base Erosion and Profit Shifting Project, OECD Publishing, 2014, http://www.oecd.org/ctp/tax-challenges-digital-economy-discussion-draft-march-2014.pdf.

[182] Internal Revenue Service, *IRS Intensifies Work on Identity Theft and Refund Fraud; Criminal Investigation Enforcement Actions Underway across the Nation,* 2014, https://www.irs.gov/uac/newsroom/irs-intensifies-work-on-identity-theft-and-refund-fraud-criminal-investigation-enforcement-actions-underway-across-the-nation.

[183] Key definitions: Placement—depositing money into the financial system, layering—distancing money from its source through a series of transactions, and integration—the commingling of money with funds in legal sectors.

[184] Wojciech Filipkowski, "Cyber Laundering: An Analysis of Typology and Techniques," International Journal of Criminal Justice Sciences (IJCJS) 3, no. 1 (2008): 15-27.

[185] National Drug Intelligence Center, Money Laundering in Digital Currencies, US Department of Justice, 2008, http://www.justice.gov/archive/ndic/pubs28/28675/28675p.pdf.

[186] Tatiana Tropina, "Fighting Money Laundering in the Age of Online Banking, Virtual Currencies and Internet Gambling," ERA Forum 15, no. 1 (June 2014): 69-84.

[187] Council of Europe, Criminal Money Flows on the Internet: Methods, Trends, and Multi-stakeholder Counteraction, Moneyval Research Report, March 2012, http://www.coe.int/t/dghl/monitoring/moneyval/Activities/MONEYVAL(2013)6_Reptyp_flows_en.pdf, 36.

[188] FATF, Money Laundering & Terrorist Financing Vulnerabilities of Commercial Websites and Internet Payment Systems, 2008, http://www.fatf-gafi.org/.

A woman looks at a map showing where eight members belonging to a New York-based cell of a global cyber criminal organization withdrew money from ATM machines. The US government charged eight individuals with using data obtained by hacking into two credit card processors in a worldwide scheme that netted some $45 million within hours, a crime prosecutors described as one of the biggest bank heists in history.
Photo credit: Reuters/Lucas Jackson.

behavior, especially if their primary goal is to provide bulletproof payment services.

The following tools can be used to facilitate illicit financial flows: online banking[189] and mobile banking;[190] electronic payment systems via unregulated financial intermediaries;[191] cryptocurrencies;[192] online services and trading

[189] Council of Europe, Criminal Money Flows on the Internet; see also Christine Victoria Thomason, "How Has the Establishment of the Internet Changed the Ways in Which Offenders Launder Their Dirty Money?" Internet Journal of Criminology, July 2009, http://www.internetjournalofcriminology.com/Thomason_Internet_Money_Laundering_July_09.pdf and Stephen J. Weaver, "Modern Day Money Laundering: Does the Solution Exist in an Expansive System of Monitoring and Record Keeping Regulations?" Annual Review of Banking & Financial Law 24, 2005: 443-465.

[190] John Villasenor, Christopher Bronk, and Cody Monk, Shadowy Figures: Tracking Illicit Financial Transactions in the Murky World of Digital Currencies, Peer-to-Peer Networks, and Mobile Device Payments, The Brookings Institution and the James A. Baker III Institute for Public Policy, August 29, 2011, http://bakerinstitute.org/media/files/Research/d9048418/ITP-pub-FinancialTransactions-082911.pdf. See also LIRNEasia & UP–NCPAG, Mobile Banking, Mobile Money and Telecommunication Regulations, 2008, http://lirneasia.net/wp-content/uploads/2008/05/Mobile-2.0_Final_Hor_EA.pdf.

[191] Jean-Loup Richet, Laundering Money Online: A Review of Cybercriminals Methods: Tools and Resources for Anti-corruption Knowledge, United Nations Office on Drugs and Crime, June 1, 2013, arxiv.org/pdf/1310.2368; see also Giulio Piller and Elvis Zaccariotto, "Cyber-Laundering: The Union between New Electronic Payment Systems and Criminal Organizations," Transition Studies Review 16, no. 1 (2009): 62-76, and Tropina, "Fighting Money Laundering in the Age of Online Banking."

[192] Danton Bryans, "Bitcoin and Money Laundering: Mining for an Effective Solution," Indiana Law Journal 89, August 29, 2013, http://ssrn.com/abstract=2317990, 1; Europol, iOCTA, and TRACFIN, Regulating Virtual Currencies, 2014, http://www.economie.gouv.fr/files/regulatingvirtualcurrencies.pdf.

platforms; and online gambling.[193] Most of these tools represent legal services and technologies that criminals can abuse because their operations exist outside of regulatory compliance and oversight. Even if some of the payments services, such as Zerocoin and Darkcoin, are known as special niche cryptocurrencies that offer total anonymity and might attract criminals,[194] they are also used for legitimate purposes and, therefore, cannot be attributed to only criminal activities.

“. . . [O]rganized crime groups will exploit big data ‘to carry out complex and sophisticated identity frauds [at] previously unprecedented levels’.”

Big Data: A Big Advantage for Criminals?

Data have always been integral to the execution of digital crime: the trade of data as a valuable illicit commodity drives the whole underground economy of cybercrime. With data becoming an asset “akin to oil in the twentieth century”[195] for legitimate businesses, the value of this commodity has also significantly increased for criminals. The more data the industry creates and stores, the more criminals are happy to consume them.[196]

To enjoy the benefits of big data, businesses tend to aggregate vast amounts of sensitive data from various sources in one place to better analyze them.[197] Such centralization also increases the value of the data for criminals and makes companies and their databases more attractive and vulnerable to cyberattacks.[198] The trade in consumer data in the legitimate economy also makes that data more vulnerable given criminals can acquire data via legal transactions. For example, in 2013 the leading global consumer credit bureau Experian inadvertently sold sensitive data on US consumers via Court Ventures, a company it acquired in 2012, to a Vietnamese identity theft ring. Data transferred to the criminals included names, addresses, Social Security numbers, birthdays, work history, driver’s license numbers, email addresses, and banking information.[199]

By exploiting the vulnerabilities of centralized data storage, criminals can develop aggressive and complex techniques to commit crimes. The acquisition of a large volume of sensitive personal data can allow for phishing schemes that target individuals rather than businesses or certain demographic groups and, therefore, are harder to detect.[200] Moreover, Europol predicts that in the future organized crime groups will exploit big data “to carry out complex and sophisticated identity frauds [at] previously unprecedented levels.”[201] Highly personalized scams can target a particular person on the basis of details from a social networking profile or from financial activity. Further development of biometrics in combination with big data might enable criminals to create false identities that could be used both digitally and in the real world.[202] All of these risks have to be taken into account when developing technical and legal responses to both offline and online crime.

[193] Filipkowski, “Cyber Laundering.” See also Council of Europe, The Use of Online Gambling for Money Laundering and the Financing of Terrorism Purposes, 2013, http://www.coe.int/t/dghl/monitoring/moneyval/activities/MONEYVAL(2013)9_Onlinegambling.pdf and Ingo Fiedler, Online Gambling as a Game Changer to Money Laundering? Institute of Commercial Law, University of Hamburg, April 30, 2013, http://ssrn.com/abstract=2261266.

[194] TRACFIN, Regulating Virtual Currencies; see also Europol, iOCTA.

[195] Raymond D. Moss, “Civil Rights Enforcement in the Era of Big Data: Algorithmic Discrimination and the Computer Fraud and Abuse Act,” March 9, 2016, Columbia Human Rights Law Review 48.1, 2016: 1.

[196] Marc Goodman, Future Crimes (New York: Knopf Doubleday Publishing Group, 2015), 137.

[197] Colin Tankard, “Big Data Security,” Network Security 2012, no. 7 (July 2012): 5–6.

[198] Jose Gutierrez, Thomas Anzelde, and Galliane Gobenceaux, Risk and Reward: The Effect of Big Data on Financial Services, Leading Trends in Information Technology, Stanford University, Summer 2014, https://web.stanford.edu/class/msande238/projects/2014/BigDataFinance.pdf, 18; Lidong Wang and Cheryl Ann Alexander, “Big Data in Distributed Analytics, Cybersecurity, Cyber Warfare, and Digital Forensics,” Digital Technologies 1, no. 1 (2015): 22-27, doi: 10.12691/dt-1-1-5, and Tankard, “Big Data Security,” 5-6.

[199] Brian Krebs, Experian Sold Consumer Data to ID Theft Service, Krebs on Security, October 20, 2013, https://krebsonsecurity.com/2013/10/experian-sold-consumer-data-to-id-theft-service/.

[200] Trend Micro, Addressing Big Data Security Challenges: The Right Tools for Smart Protection, 2012, http://www.trendmicro.de/media/wp/addressing-big-data-security-challenges-whitepaper-en.pdf, 4.

[201] Europol, Exploring Tomorrow’s Organized Crime, 2015.

[202] Ibid.

Illegal Profits and Big Data: New Challenges, New Opportunities?

Prevention, Detection, and Disruption of Illicit Financial Flows

The banking industry and law enforcement agencies employ various tools to investigate crime and comply with regulations, such as the Know Your Customer requirement.[203] These tools range from anti-money-laundering software for financial industries to special equipment for digital crime investigations and electronic evidence collection.

Every year, software vendors offer industry and law enforcement agencies cutting-edge technical solutions for fighting financial crime. Some of them, like Egmont Secure Web and FIU.net, are specifically tailored to tackle the problem of illicit financial flows by managing requests for financial intelligence sharing from abroad and providing secure information exchange for this purpose.[204] Technology is employed to analyze data from beneficial ownership databases—databases that collect information about companies' owners and organizational structures and link them together—and to obtain electronic records about transaction trails to detect corruption and tax evasion by connecting seemingly unrelated transactions and activities.[205]

However, due to the increasing volume of data flows, neither law enforcement nor private companies can continue to monitor suspicious behavior using traditional tools based only on linear data.[206] Therefore, big data analytics, which can process and analyze nonlinear datasets and link together seemingly disconnected data, is considered a powerful "weapon of choice."[207] Big data tools have been revolutionary[208] in replacing or complementing manual techniques, connecting previously disconnected dots, and enabling quick responses to threats—all of which makes it easier to react before malicious activity has caused significant damage.[209] Big data analytics is able to predict security breaches by identifying abnormalities and quickly processing large amounts of linear and nonlinear data from different sources.[210] Moreover, big data solutions can not only stop criminal acts, they also play a significant role in predicting them before they occur, thus facilitating new, proactive approaches to fighting illicit financial flows.[211]

Big data analytics is also addressing the cross-border elements of illegal financial flows. Analytics makes data sharing between law enforcement agencies faster and more efficient and helps transnational crime investigations by identifying patterns.[212] Big data tools also help with mapping and visualization[213] to provide a broader picture of the illicit financial flows and identify affected geographical areas, industry players, channels, and suspects.[214]

The benefits of using big data to tackle crime and illicit money transfers have become obvious in recent years. Old investigation tools cannot analyze the ever-growing amounts of unstructured data. Thus, big data tools have been implemented in different areas and used by governments, private industry,

[203] Know Your Customer is a process implemented by banks to obtain information about their customers' identities to ensure that the banking system is not misused. In many countries, anti-money laundering regulations require that banks implement this process.

[204] TRACFIN, Annual Analysis and Activity Report 2013, http://www.economie.gouv.fr/files/ra_tracfin_anglais_2013.pdf.

[205] Tatiana Tropina, Do Digital Technologies Facilitate Illicit Financial Flows, World Bank, 2016, http://documents.worldbank.org/curated/en/896341468190180202/pdf/102953-WP-Box394845B-PUBLIC-WDR16-BP-Do-Digital-Technologies-Facilitate-Illicit-Financial-Flows-Tropina.pdf.

[206] Heather Adams, Fighting Financial Crime with Data, Accenture, 2015, https://www.accenture.com/t20160519T222110w/us-en/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Industries_6/Accenture-Fighting-Financial-Crime-with-Data.pdf, 4.

[207] Deloitte, Insight on Financial Crime: Challenges Facing Financial Institutions, 2014, http://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-cm-insight_on_financial_crime.pdf, 5.

[208] Europol, Exploring Tomorrow's Organized Crime, 2015, 43.

[209] Executive Office of the President, Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights, United States Government, 2016, https://www.whitehouse.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf; Joe Goldberg, "Tackling Unknown Threats," Network Security 12, 2014: 16-17.

[210] Digital Reasoning, Unstructured Data: A Big Deal in Big Data, http://www.digitalreasoning.com/resources/Holistic-Analytics.pdf, 2. See also Wang and Alexander, "Big Data in Distributed Analytics."

[211] Deloitte, Insight on Financial Crime: Challenges Facing Financial Institutions, 2014, http://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-cm-insight_on_financial_crime.pdf; Trend Micro, Addressing Big Data Security Challenges, 5; Wang and Alexander, "Big Data in Distributed Analytics"; and Jill Coster van Voorhout, Tesse Alleblas, and Ting Zhang, Curbing Illicit Financial Flows: The Post-2015 Agenda and International Human Rights Law, The Hague, November 2015, http://www.thehagueinstituteforglobaljustice.org/wp-content/uploads/2015/11/PB8-Illicit-Financial-Flows.pdf, 10.

[212] Houses of Parliament, Big Data, Crime, and Security, POSTnote, no. 470 (July 2014), researchbriefings.files.parliament.uk/documents/POST-PN-470/POST-PN-470.pdf, 3.

[213] One example of such an infographic can be found at Dawson and Li, *Top 20 Countries Losing Money from Illicit Financial Flows*, Thomson Reuters Foundation*,* 2013, http://news.trust.org//item/20131211124740-udist/.

[214] Van Voorhout, Alleblas, and Zhang, Curbing Illicit Financial Flows, 10. See also Shaun Hipgrave, "Smarter Fraud Investigations with Big Data Analytics," Network Security 12, 2013: 8.

nongovernmental organizations, and journalists to detect and investigate illegal transactions.

How Is Big Data Being Used to Tackle Illicit Financial Flows?

Financial Industry

In the age of digital crime, holistic approaches to crime detection have also been embraced by the financial industry, which suffers from increasing vulnerability to fraud and is a vehicle for money laundering. While facing significant financial losses from fraudulent activities, the financial industry also bears the largest burden of regulatory compliance. In most countries, banking regulations require financial intermediaries to share information with regulators and law enforcement about suspicious transactions even if the illegality of the act has not been proven.[215]

Myriad bank transactions happen every day. Traditional systems that are based on the analysis of structured data, such as credit card transactions, and on small samples of data cannot tackle the problem of detecting complex illegal schemes.[216] But, big data analytics can use structured and unstructured raw data from different sources, such as geolocation data and those from mobile devices and social media, to detect fraudulent activities, unearth hidden connections between accounts, and track the relationship between the sources and beneficiary.[217] As a result, big data analytics is replacing traditional approaches that rely on "red flag" alerts and linear data analysis with predictive models based on processing large volumes of data, such as transactions history and payment activity patterns, in real time.[218]

Likewise, regulators are also using big data analytics to carry out predictive analysis of money laundering in the financial industry. Big data analytics are being used by financial institutions to review successful investigations, identify indications of money laundering, and develop automated rules and universal templates for the industry to better fight the practice. Furthermore, big data tools are helping collect more detailed information from the industry and analyze it in more advanced ways.[219]

Big data analytics are also helping detect the misuse of new types of payments, especially virtual currencies based on blockchain technology. Despite the great degree of anonymity blockchain offers, big data tools can make it possible to track and match information on certain types of transactions, making sure that actions are legitimate and genuine. Given the recent calls to consider options for regulating blockchain,[220] big data analytics could be employed not only so regulators and enforcement agencies can detect illicit financial flows via blockchain, but also to encourage the voluntary creation of more secure and trusted digital currencies and payment systems in cases when no effective regulatory frameworks are found.

Trade-Based Money Laundering

Similarly, big data tools help detect trade-based money laundering, which includes over- and under-invoicing, multiple invoicing, over- and under-shipment, and other techniques that allow criminals to move funds across borders in the form of goods. The use of automated text analytics combined with web-analysis and web-crawling is considered to be a revolutionary development to ensure transparency in global trade.[221]

Governments and the private sector use big data algorithms to analyze both structured and unstructured transactions data. When combined with multiple records from different countries and institutions, big data can uncover suspicious patterns such as mismatches in corresponding documentation, shipment routes, and details; discrepancies between goods descriptions and shipment documents; multiple deposits; and other

[215] Stavros Gadinis and Colby Mangels, "Collaborative Gatekeepers," Wash. & Lee L. Rev. 73, no. 2 (2016), http://scholarlycommons.law.wlu.edu/wlulr/vol73/iss2/6, 802.

[216] Gutierrez, Anzelde, and Gobenceaux, Risk and Reward, 10; IBM, Combat Credit Card Fraud with Big Data, 2013, http://www.intel.de/content/dam/www/public/us/en/documents/white-papers/combat-credit-card-fraud-with-big-data-whitepaper.pdf, 2.

[217] Bashyam Selvaraj, Combating Fraud and Money Laundering: How the Financial Services Industry Can Leverage Big Data, Tata Consulting Services, 2015, http://www.tcs.com/SiteCollectionDocuments/White-Papers/Combating-Fraud-Money-Laundering-0415-1.pdf, 1-3; Intel, Reduce Money Laundering Risks with Rapid, Predictive Insights, Solution Brief, 2015, http://www.intel.de/content/dam/www/public/emea/xe/en/documents/financial-services/final-aml-solution-brief.pdf, 2.

[218] Selvaraj, Combating Fraud and Money Laundering, 3. See also Helena Forest, Evelyn Foo, Donya Rose, and Dmitriy Berenzon, Big Data: How It Can Become a Differentiator, Deutsche Bank, 2015, http://cib.db.com/insights-and-initiatives/flow/35187.htm, 12; Hipgrave, "Smarter Fraud Investigations," 8, and Daniel Mayo, Assessing the Role of Big Data in Tackling Financial Crime and Compliance Management, OVUM, 2016, http://www.oracle.com/us/industries/financial-services/fs-big-data-fccm-wp-2861557.pdf, 8.

[219] Such tools have been employed in the United States by FINSEC. See Holly Gilbert, *Treasury Department Using Advanced Analytics to Help Detect, Prevent Money-Laundering,* 2013, http://www.predictiveanalyticsworld.com/patimes/treasury-department-using-advanced-analytics-to-help-detect-prevent-money-laundering/1043/.

[220] As mentioned earlier in this paper, FinCEN in the United States and FATF have called for monitoring the regulatory issues and possibly creating regulatory frameworks for digital currencies.

[221] John A. Cassara and Chip Poncy, Trade-Based Money Laundering: The Next Frontier in International Money Laundering Enforcement, Wiley, 2015, 164.

issues.[222] Since the trade finance business relies on paper documents related to specific transactions, big data analytics, especially text analytics, can effectively tackle trade-based money laundering.[223]

Box 4.3. Big Data to Tackle Trade-Based Money Laundering in Developing Countries

In November 2016, DC-based nonprofit Global Financial Integrity launched a new database tool—FTrade—that is geared toward helping developing countries. It can analyze prices in real time and measure trade misinvoicing risks for eighty thousand goods categories.[224]

Terrorist Financing

Tracking terrorist financing is yet another area where big data analytics can be useful. Some of the national and international efforts in this field have already been based on using large volumes of data to track terrorist money. For example, under the European Union-US Terrorist Finance Tracking Program, data on international bank transfers are passed, under the management of Europol, to the US Treasury for further assessment.[225] Recently, Danish journalists were able to establish links between terrorism financing and value-added-tax (VAT) refund scams by using big data analytics instruments: different datasets collected from public records were scraped and compiled to identify critical nodes and patterns, which were further verified by journalists.[226] The analysis resulted in a documentary, which was broadcast in Denmark, and sparked the launch of a further investigation by the Danish Security and Intelligence Service.[227]

In the United States, FinCEN uses advanced analytics tools to detect terrorist financing. The data gathered by FinCEN—via special rules that help identify transactions by particular terrorist organizations—generate matches in advanced data analytics systems for review and exploration. The results are passed to law enforcement and the intelligence community for further investigation.[228] Furthermore, in 2016 FinCEN proposed a rule that would require crowdfunding portals to enact policies and procedures to prevent money laundering and terrorist financing.[229] This rule would extend the application of big data analytics to include monitoring crowdfunding for signs that it is being used to finance terrorism.

Tax Crimes

Governments and international organizations are currently trying to determine how big data can best tackle offshore tax evasion. Successful examples already exist in this field. For instance, the United Kingdom's tax and customs authority has been effectively using big data analytics to tackle the problem of tax fraud. Likewise, the Internal Revenue Service (IRS) in the United States is using big data analytics—quantitative algorithms and statistical models—to detect fraud and taxpayer identity theft.[230] Additionally, the OECD has developed special programs to tackle tax avoidance and base erosion and profit shifting.

Box 4.4. Big Data to Fight Tax Fraud: A United Kingdom Case Study

The United Kingdom's tax and customs authority (Her Majesty's Revenue & Customs, or HMRC) employs the big data tool Connect to detect tax evasion and tax fraud. Connect makes it possible to bring together and analyze billions of pieces of HMRC internal data. It performs searches of information, which would otherwise be difficult to find, to elicit patterns and connections that uncover crime. HMRC reported that between April 2013 and April 2014 it was able to recover £2.6 billion by using this technology, with an initial investment of £45 million (including five years of running costs).[231]

[222] PwC, Goods Gone Bad: Addressing Money-Laundering Risk in the Trade Finance System, January 2015, http://www.pwc.com/us/en/risk-assurance-services/publications/assets/pwc-trade-finance-aml.pdf.

[223] Ibid., 13.

[224] Global Financial Integrity, "GFI Launches Database—GFTrade—to Help Developing Countries Generate Millions in Additional Public Revenue," November 9, 2016, http://www.gfintegrity.org/press-release/gfi-launches-database-gftrade-to-help-developing-countries-generate-millions-in-additional-public-revenue/.

[225] Statewatch, Note on Big Data, Crime, and Security: Civil Liberties, Data Protection, and Privacy Concerns, April 3, 2014, http://www.statewatch.org/analyses/no-242-big-data.pdf, 2.

[226] EurActive, Big Data Revolutionizes Europe's Fight against Terrorism, 2016, https://www.euractiv.com/section/digital/news/big-data-revolutionises-europes-fight-against-terrorism/; see also Global Editors Network, "The VAT Hustlers," 2016, http://community.globaleditorsnetwork.org/content/vat-hustlers-0.

[227] The Local DK, "Terror Suspects Tied to VAT Scam in Denmark," January 25, 2016, http://www.thelocal.dk/20160125/terror-suspects-tied-to-financial-fraud-in-denmark.

[228] FinCEN, *Statement of Jennifer Shasky Calvery*.

[229] C. Todd Gibson, Michael McGrath, and Ken Juster, *FinCEN Proposal to Impose AML Obligations on US Funding Portals,* K&L Gates, 2016, https://www.fintechlawblog.com/2016/05/fincen-proposal-to-impose-aml-obligations-on-u-s-funding-portals.

[230] Charles S. Clark, "IRS and SEC Detect Fraud Patterns in Heaps of Data," Government Executive, October 16, 2012, http://www.govexec.com/technology/2012/10/irs-and-sec-detect-fraud-patterns-heaps-data/58816/.

[231] United Kingdom Houses of Parliament, "Big Data, Crime, and Security," Postnote, July 2014, 3.

Big data analytics can help law enforcement agencies with criminal investigations, allowing them to deal with large amounts of data to identify connections between seemingly unrelated pieces of information.
Photo credit: Reuters/Jonathan Ernst.

Law Enforcement: Crime Prevention and Crime Control

Big data tools equip law enforcement agencies with the powerful analytical processes that improve both proactive and reactive approaches to policing. Such tools are helpful not only in online crime investigations, where law enforcement has to deal with the growing amount of data that need to be analyzed, but also in investigating any complex situations, like organized crime, where it is necessary to identify connections between seemingly unrelated pieces of information. Big data analytics can be used to store, combine, and match all existing information, categorize content, and establish correlations. Furthermore, big data tools are used to identify risks, understand crime patterns, and share information between agencies.[232]

Big Data and Big Challenges

While the promise of big data analytics has not yet been fully delivered, big data tools are being used successfully. Nevertheless, both governments and the private sector must consider many factors before fully enjoying the benefits that big data tools bring to the prevention, detection, and investigation of crime and illegal money transfers.

Big Data and Human Capacity

While able to bring significant improvements to tackling illicit financial flows, big data tools alone are not the answer; they are just a part of the

[232] Justin Heinze, “Fighting Crime with Data: How Law Enforcement Is Leveraging Big Data Analytics to Keep Us Safe,” Better Buys, 2014, https://www.betterbuys.com/bi/fighting-crime-with-data/; “How Big Data Analytics Can Be the Difference for Law Enforcement,” SAS, https://www.sas.com/en_us/insights/articles/risk-fraud/big-data-analytics-for-law-enforcement.html; Abdullahi Muhammed, “A Look into Big Data Applications for Law Enforcement,” Smart Data Collective, 2016, http://www.smartdatacollective.com/oxygenmat/382813/look-big-data-applications-law-enforcement.

response.[233] Even the most sophisticated technical solutions require humans to use the results and determine future actions.[234] While big data tools enable people to perform analyses that can identify illegal financial flows, they also rely on people to ask better questions, see the broader picture, establish links, find correlations, and, ultimately, make decisions.[235]

The human factor is especially important given the danger of wrong and misleading data and the possibility of incorrectly interpreting data. It is critical to ensure the quality, authenticity, and integrity of data for big data analytics, but mistakes can occur due to human error.[236] Therefore, law enforcement agencies[237] and private industry[238] must work on capacity building and developing specialized knowledge in advanced data analytics to better ensure that the data being analyzed are sound and that the analysts can interpret results correctly.

Box 4.5. Bitcoin and Money Laundering

In January 2016, the Dutch police arrested ten people in conjunction with an international investigation into a money laundering scheme that used a cryptocurrency—bitcoin—to launder up to twenty million euros from online drug deals. Some of the suspects were operating as bitcoin traders who had acquired the currency through the illegal trade in drugs; others were involved in exchanging the cryptocurrencies for euros to withdraw them from ATMs (automated teller machines). The alarm that led to the investigation and subsequent arrests was raised by the banks, because eventually the criminals combined the use of cryptocurrencies with traditional banking and used their bank accounts to deposit large sums of money to then quickly withdraw from ATMs.[239]

Big Data Privacy Concerns and Safeguards

The principal challenges for big data solutions are the following: 1) addressing concerns about the vulnerability of databases containing personal data[240] and 2) ensuring the legality, necessity, and proportionality of analyzing data to tackle criminal activity.[241] Privacy issues are very important for the industry given the increased use of big data analytics to prevent malicious activity. Some industry players have already recognized ethical and privacy risks. According to Deutsche Bank, "one bank removed face recognition algorithms from its set of analytics, because it did not even want to be seen as being able to use it."[242] Nevertheless, there is an ongoing debate about how industry can help alleviate these challenges.

In the age of big data, addressing privacy concerns and maintaining appropriate security safeguards are also of the utmost importance for law enforcement and intelligence agencies. Data processing for the purposes of crime prevention and criminal investigation in many countries is subject to strict safeguards, checks, and balances. For this reason, law enforcement must be cautious when implementing big data solutions to avoid overstepping legal boundaries.

Big Data Tools and Capacity Building in Developing Countries

Illicit financial flows have devastating effects on developing countries. While big data analytics can help tackle the problem more effectively, the lack of regulatory and enforcement instruments in place to control financial crime and tax evasion will not be fixed by technical solutions. Therefore, in addition to technical tools, developing countries need to institute coherent policies, regulatory frameworks, and human capacity building. One of the biggest challenges is ensuring big data solutions can tackle all vulnerabilities in financial systems that enable illicit financial flows in developing countries.

[233] Trendmicro, *Addressing Big Data Security Challenges: The Right Tools for Smart Protection*, White Paper, 2012, http://www.trendmicro.de/media/wp/addressing-big-data-security-challenges-whitepaper-en.pdf; Surfwatch, Big Data, Big Mess, 2.

[234] Articol Bănărescu, "Detecting and Preventing Fraud with Data Analytics," Emerging Markets, Queries in Finance and Business, Procedia Economics and Finance 32, 2015: 1832–1833.

[235] Conrad Constantine, "Big Data: An Information Security Context," Network Security, January 2014, 19. See also Surfwatch, Big Data, Big Mess, 3.

[236] Forest, Foo, Rose, and Berenzon, Big Data, 20.

[237] Europol, Exploring Tomorrow's Organized Crime, 43.

[238] Forest, Foo, Rose, and Berenzon, Big Data, 21.

[239] "Ten Arrested in Netherlands over Bitcoin Money-Laundering Allegation," *Guardian*, January 20, 2016, https://www.theguardian.com/technology/2016/jan/20/bitcoin-netherlands-arrests-cars-cash-ecstasy; Daniel Dob, "Dutch Police Arrests 10 Men for Bitcoin Money Laundering," The Merkle, January 20, 2016, http://themerkle.com/dutch-police-arrests-10-men-for-bitcoin-money-laundering/; and Organized Crime and Corruption Reporting Project, "10 Arrested in Netherlands in Bitcoin Operation," January 22, 2016, https://www.occrp.org/en/daily/4841-10-arrested-in-netherlands-in-bitcoin-operation.

[240] Wang and Alexander, "Big Data in Distributed Analytics"; Neil Richards and Jonathan King, "Three Paradoxes of Big Data," 66 Stanford Law Review Online 41, September 3, 2013; Forest, Foo, Rose, and Berenzon, Big Data; and Statewatch, "Note on Big Data."

[241] Houses of Parliament, Big Data, Crime and Security, 1.

[242] Forest, Foo, Rose, and Berenzon, Big Data, 21.

"Follow the Money": The Nexus of Digital Technologies and the Law

Big data tools could potentially bridge the technology gap between law enforcement agencies and sophisticated criminals. However, big data solutions do not come in a vacuum. Big data tools may solve technical problems by tracing, reporting, and predicting crime, but there are complex legal problems associated with tackling illegal money that existed long before digital technologies enabled new illicit financial flows.

Digital criminal activities can easily bypass national legal frameworks and borders that national regulators and law enforcement agencies cannot. National regulators and law enforcement agencies can enforce only the laws of the country in which they operate and they can do so only within their own national borders; therefore, they must rely on mutual legal assistance to stop criminal activities. In other words, though technological solutions, even those as promising as big data analytics, can provide powerful crime-fighting equipment, they do not fix—or bridge—all legal gaps. As a result, it will be impossible to fully harness big data's ability to fight crime and money laundering without concurrently facilitating cross-border data flows, investigations, and the exchange of electronic evidence; harmonizing regulatory and legal frameworks; and developing procedural tools and common digital forensics standards.

Lastly, the existence of thousands of stakeholders in the digital economy calls for public-private cooperation between industry and governmental bodies. While regulated intermediaries, such as entities in the financial industry, can certainly employ big data or other technological tools to better comply with anti-money laundering regulations or to protect themselves from financial fraud, there are thousands of unregulated payment providers and other intermediaries outside the scope of compliance procedures that lack incentives to contribute to the effort of mitigating illicit financial flows. Thus, it is important to find those incentives and promote collaborative voluntary approaches. Good solutions should be multi-faceted and include proper national legal frameworks; mutual legal assistance instruments able to cope with the speed of information transfers; frameworks for self-regulation, public-private cooperation, and raising awareness; and a commitment to the ongoing education of users about how to avoid crimes like identity theft.

Recommendations

- Governments, law enforcement, and private industry should employ big data analytical tools to tackle illicit financial flows; these tools have significant potential to develop solutions that would complement all previously isolated efforts to fight financial crime.
- Since big data analytics requires people to analyze results and determine appropriate actions, governments and private industry should recognize that one of the keys to success is building the human capacity to best use these innovative tools.
- Using big data tools requires governments and industry to address privacy considerations; safeguarding people's privacy should be an integral part of using big data analytics.
- Big data analytics requires proper legal frameworks that address trans-border criminal investigations, mutual legal/regulatory assistance, and compliance at the national level. To enjoy the benefits of big data, governments must implement proper laws and regulations surrounding its use and be ready to update them in the face of unforeseen technological challenges.
- Given that both governments and industry face the same technical, privacy, and ethical challenges in implementing big data tools for tracing illicit financial flows, there should be an ongoing dialogue and partnership between government and industry to build trust, share information, and develop industry standards.
- Using existing and new big data tools should be considered part of an ongoing process and long-term comprehensive strategy to tackle the problem of illicit financial flows. This multi-faceted strategy should comprise both reactive and proactive approaches and include technical and legal tools, public-private cooperation, and future risks analysis.

Conclusion

No single technical or legal solution, or any combination, will completely solve the problem of illicit financial flows. Illicit profit flows and crime will possibly exist as long as humanity does. However, big data analytics, when implemented correctly, can be a game changer for tackling financial crime and money laundering: technology can empower law enforcement agencies with the tools that enable them to both react to complex crime and money laundering and predict it. Nevertheless, to fully benefit from big data solutions, tools need to be complemented by proper legal frameworks, human capacity building, and working mechanisms to support cross-border crime investigations. Ultimately, any technology, no matter how revolutionary it could be, should be considered one part of a long-term strategy to tackle crime and abuse of the financial system—a strategy that should not only be able to address the current risks, but anticipate future ones.