

# **A review of online business regulatory framework to reduce IFF in Bangladesh**

**SONY, M M ABDULLAH AL MAMUN**

*ABSTRACT Illicit Financial Flow (IFF) is a key development challenge all over the world. In developing countries, though IFF may take place in different ways, but over the past couple of years IFF via the digital ecosystem has been demanding a rethink of the existing legal structure. For instance, in Bangladesh, the fastest developing country, by today about five leading e-commerce companies have been accused of fraud mostly in supply chain management and also accused of money laundering issues. Therefore, the Bangladesh government has adopted Digital Commerce Guidelines. Since these e-commerce scams take place frequently, this raises the question of the effectiveness of this existing legal structure in Bangladesh and how the same legal framework can meet the challenge of IFF via digital platform. With the help of the comparative method, the research has tried to address these gaps in academic literature from a qualitative approach. This study has indicated that a flaw in Bangladesh's present regulatory system is the lack of legislative directions on how to supervise excessive discounts or predatory pricing. Finally, no cross-border e-commerce rules or recommendations have been established under the present legal regulatory framework. As a result, it is suggested that these flaws in the current policy be reconsidered to reduce IFF. Overall, the findings of this study will assist policymakers in defining additional actions aimed at reforming a robust digital regulatory environment.*

*KEYWORDS Digital, Commerce, Supervision, Legal system, Illegal finance, Bangladesh*

## **1. Introduction**

In the wake of the coronavirus pandemic, business and commerce on the digital platform have gained more popularity than ever before. Evidence of this can be found in the report of UNCTD (2021)<sup>1</sup> which has shown that global online retail sales increased from 14 to 19 percent between 2018 and 2020. Likewise, a dramatic increase in these platforms' growth has been addressed by

---

<sup>1</sup> UNCTD, "Covid-19 and E-Commerce: A Global Review," in *United Nations Conference on Trade and Development*, Geneva: UNCTAD Technical Notes on ICT for Development, 2021.

Alcedo et al. (2022)<sup>2</sup> after analyzing global e-trade and services data in the period between pre-pandemic and pandemic times. Observing such a scenario OECD (2022)<sup>3</sup> has drawn policymakers' attention to the need to rethink the changing nature of trade and commerce structure, since everything from luxury goods and services to daily necessary products is available online even in the third world country.

Linked to this statement, an estimation has also found that in South Asia alone the online retailer market value would be worth \$90 billion and the growth will continue from 6.0% to 11.2% between 2020 and 2025.<sup>4</sup> In a similar vein, another popular organization Statista (2022)<sup>5</sup> has projected that the market share of online business by the end of 2022 only in Bangladesh, a fast-growing South Asian country, is going to be worth \$8,030 million and the number of beneficiaries will have grown to 75.5 million by the end of 2025. The mean revenue per user is also expected at \$136.72.<sup>6</sup>

However, over the past few years, several scholars' development organizations have also been stressing the question as to whether these digital platforms are facilitating the illicit financial flow (IFF) or not. For instance, focusing on the relationship between IFF and digital technologies (DT), Tropina (2016)<sup>7</sup> - in a World Bank fact sheet - highlighted some areas of the close association between these two umbrella terms. Illegal procurement of money is one of the most important areas of IFF and DT relationship identified by Tropina (2016)<sup>8</sup>, which has been produced and reproduced by illegal online markets and the lack of proper policy measures. Moreover, these transforming platforms also make the room for a number of opportunities for fraud, corruption, tax evasion, and other criminal activities (Kabir,<sup>9</sup> Tropina<sup>10</sup>). For example, Evaly, one of the popular e-commerce platforms in Bangladesh, has

---

<sup>2</sup> Joel Alcedo, Alberto Cavallo, Bricklin Dwyer, Prachi Mishra, and Antonio Spilimbergo, "E-Commerce During Covid: Stylized Facts from 47 Economies," (Cambridge: National Bureau of Economic Research, 2022).

<sup>3</sup> OECD, "Coherent Policies for Combatting Illicit Financial Flows," Framework for Policy Coherence for Sustainable Development: Thematic Module on Illicit Financial Flows [SG/PCD(2016)3], 2016, <http://www.un.org/esa/ffd/ffd-follow-up/inter-agency-task-force.html>.

<sup>4</sup> Ethan Cramer-Flood and Benjamin Silverman, "Southeast Asia Ecommerce Forecast," 2022, <https://www.emarketer.com/content/southeast-asia-ecommerce-forecast-2022>.

<sup>5</sup> Statista, "Digital Markets eCommerce Bangladesh," 2022, <https://www.statista.com/outlook/dmo/ecommerce/bangladesh>.

<sup>6</sup> Ibid.

<sup>7</sup> Tatiana Tropina, "Do digital technologies facilitate illicit financial flows?," World Bank, 2016, <https://openknowledge.worldbank.org/handle/10986/23803>.

<sup>8</sup> Ibid.

<sup>9</sup> Md. Adnan Kabir, "A Legal Analysis on Resolving Recently Growing Online Business Frauds in Bangladesh," International Conference on Human Rights and Business Law, Chittagong, 2022.

<sup>10</sup> Tropina, "Do digital technologies facilitate illicit financial flows?"

been accused of committing fraud in its supply chain management.<sup>11</sup> In Bangladesh, another piece of evidence linking e-commerce business and avoidance of customs tax has been presented by Islam (2020).<sup>12</sup>

Further, these new digital platforms as well as a new form of doing business online without proper regulation do not only act as a facilitator of illegal profits and fake e-commerce companies but also help to aggregate illicit funds in offshore accounts and offshore online businesses.<sup>13</sup> Aside from this, Tropina has anticipated, if online money transfers like mobile banking, electronic payments, cryptocurrencies, e-commerce providers, and online gambling services work combinedly, then several potential doors would be open for outlawed sources of money and for transmitting money from lawful sources in an unauthorized manner.<sup>14</sup> In line with this view, Joveda et al. (2019)<sup>15</sup> have speculated whether Bangladeshi Banking Industries can tackle cyber laundering in the existing legal framework. So, such questions generally urge the policymakers of third world countries to rethink their existing policies in the wake of this new industrial development.

Since, over the past couple of years several fraud cases, like Orange, Dhamaka, Evaly, Qcoom, Adyan Mart, and Aleshamart, have been discovered in Bangladesh associated with an e-commerce business. Through an unofficial source, it has been speculated that these organizations might have siphoned off \$152 million from Bangladesh.<sup>16</sup> Therefore, tackling the challenge of this new digital ecosystem in a new form of legal structure and regulatory framework has become a pressing need in Bangladesh.

The importance of regulatory frameworks for a state is not new. The effectiveness of the state-owned online regulatory structure has been highlighted by different scholars. For instance, Larionova and Shelepov (2021, 23) have stated that,

*... A window of opportunity was opened in 2020, not only to implement the G20's 2008 pledge to reform the international financial and economic architecture, but also to build a new digital economy governance system, ensuring that emerging*

---

<sup>11</sup> Farrukh Uddin, "Supply chain performance scandals of e-commerce industry: qualitative evidence from Bangladesh," *North American Academic Research* 4, no. 3 (2021): 293–308.

<sup>12</sup> Tanbirul Islam, *Tax Evasion by E-Commerce Businesses in Bangladesh*. Ontario: Brock University, 2020, <https://books.google.hu/books?id=1BZxzwEACAAJ>.

<sup>13</sup> Tropina, "Do digital technologies facilitate illicit financial flows?"

<sup>14</sup> Ibid.

<sup>15</sup> Nahid Joveda, Md. Tarek Khan, and Abhijit Pathak, "Cyber Laundering: A Threat to Banking Industries in Bangladesh: In Quest of Effective Legal Framework and Cyber Security of Financial Information." *International Journal of Economics and Finance* 11, no. 10 (2019): 54–65.

<sup>16</sup> Zia Chowdhury and Sakhawat Prince, "E-commerce scams: Now finger pointed at Foster for laundering Tk1,300cr," *The Business Standard*, 2021, <https://www.tbsnews.net/economy/e-commerce-scams-now-finger-pointed-fosterlaundering-tk1300cr-311992>.

*markets and developing countries have a voice in decision-making commensurate with their weight in the global economy.*<sup>17</sup>

Notwithstanding that, Larionova and Shelepov (2021) have highlighted the importance of a regulatory framework in Multilateral Global Governance, but it is also important at the national level, especially for protection from IFF.<sup>18</sup> The hints of it can be found in a policy brief of the CAREC (2020) institute, where they have demonstrated some key policy issues of the digital regulatory framework for member states to link with international channels safely.<sup>19</sup> To do so, this institute emphasizes some special issues as a key digital e-commerce regulatory framework, like authenticating text and transacting parties, promoting privacy, preventing cybercrime and protecting consumers, how to follow the leading international trends, and what should be done, while expressing concerns about the ability of commercial and public actors to make safe decisions, as well as the ability of some member states to administer an effective regulatory environment (CAREC, 2020).<sup>20</sup> Similar characteristics are also found in the European Union's (EU) digital economic affairs and, by providing such a strong regulatory structure, the EU is providing a safe e-commerce platform for its member states (Kwilinski et al. <sup>21</sup>; Lodder and Murray<sup>22</sup>; Lone et al. <sup>23</sup>).

Howsoever, coming back to Bangladesh's case again, over the past couple of years a significant problem of fraud and money laundering cases has emerged related to online business, which raises the question of the usefulness of existing online regulatory frameworks. Besides, beyond doubt, this existing stature is also vulnerable to accelerating IFF in Bangladesh. Against such a background this study has been designed to assess the effectiveness of Bangladesh's online regulatory framework for minimizing illicit financial flow in a critical manner by addressing two most important questions. Namely, what are the strengths and weaknesses of the existing e-commerce regularity framework in relation to minimizing the IFF of Bangladesh?

---

<sup>17</sup> Marina Larionova and Andrey Shelepov, "Emerging Regulation for Digital Economy: Challenges and Opportunities for Multilateral Global Governance." *International Organisations Research Journal* 16, no. 1 (2021): 29–63.

<sup>18</sup> Ibid.

<sup>19</sup> CAREC, "Regulatory Framework for e-Commerce Development in CAREC," T. C. Institute, 2020, <https://www.carecinstitute.org/wp-content/uploads/2020/04/2-CI-Policy-Brief-e-Commerce-Framework-in-CAREC-25-Apr-2020.pdf>.

<sup>20</sup> Ibid.

<sup>21</sup> Aleksy Kwilinski, Ruslan Volynets, Inna Berdnik, Mykhailo Holovko, and Pavlo Berzin, "E-Commerce: Concept and Legal Regulation in Modern Economic Conditions," *Journal of Legal, Ethical Regulatory Issues* 22 (2019): 1–6.

<sup>22</sup> Arno R. Lodder and Andrew D. Murray (eds.), *EU Regulation of E-commerce: A Commentary*, (Cheltenham: Edward Elgar Publishing, 2017).

<sup>23</sup> Sara Lone, N. Harboul, and Jesse Weltevreden, "2021 European E-commerce Report," 2021, [https://pure.hva.nl/ws/files/23594824/European\\_Ecommerce\\_Report\\_2021.pdf](https://pure.hva.nl/ws/files/23594824/European_Ecommerce_Report_2021.pdf).

## 2. Illicit Financial Flow (IFF)

In academia, no specific definition has been found to characterize IFF. However, international development organizations like IMF, OECD, WB, and UN use this umbrella term widely to denote national as well as cross-border illegal monetary transactions. Nevertheless, to understand IFF, it is important to know what is meant by illicit finance. When discussing illicit finance Chowla and Falcao (2016, 2) wrote,

*Illicit financial flows are the subset of illicit finance that crosses borders. The scope of all illicit finance will clearly be larger than the scope of illicit financial flow, as not all illicit finance will cross borders. Domestic tax evasion, criminal activity and corruption are significant and impact on the ability of countries to raise the finance needed to investment in sustainable development.*<sup>24</sup>

Following Chowla and Falcao's (2016) opinion, illicit finance can be perceived as finance that is procured illegally within a nation. In line with this opinion, the IMF defines the term IFF as, "...the movement of money across borders that is illegal in its source (e.g. corruption, smuggling), its transfer (e.g. tax evasion), or its use (e.g. terrorist financing)" (IMF, 2021).<sup>25</sup> Similarly, WB (2017) stated that,

*... a powerful and constructive umbrella to bring together previously disconnected issues. The term emerged in the 1990s and was initially associated with capital flight. It now generally refers to cross-border movement of capital associated with illegal activity or more explicitly, money that is illegally earned, transferred or used that crosses borders.*<sup>26</sup>

Gaining knowledge from such definition, Reuter (2017) has highlighted five important sources of IFF in a nation which include, bribes, tax evasion, criminal enterprise earnings, corporate profit shifting, and currency regulation evasion.<sup>27</sup> Besides, bulk cash smuggling, shell corporations, informal value transfer systems, and trade-based money laundering were also identified as the wider channel for these financial movements.<sup>28</sup> In a similar vein, according to WB (2017) a cash flow can be IFF only if it is procured illegally (e.g., corruption,

---

<sup>24</sup> Peter Chowla and Tatiana Falcao, "Illicit Financial Flows: Concepts and Scope," *Interagency Task Force* (2016): 1–20.

<sup>25</sup> IMF, "The IMF and the Fight Against Illicit and Tax Avoidance related Financial Flows," International Monetary Fund, Retrieved June 2 from 2021, <https://www.imf.org/en/About/Factsheets/Sheets/2018/10/07/imf-and-the-fight-against-illicit-financial-flows>.

<sup>26</sup> WB, "Illicit Financial Flows (IFFs)." The World Bank, <https://www.worldbank.org/en/topic/financialsector/brief/illicit-financial-flows-iffs>.

<sup>27</sup> Peter Reuter, "Illicit Financial Flows and Governance: The Importance of Disaggregation," *Governance the Law, Background paper for World Development Report 2017* (2017): 1–33.

<sup>28</sup> Ibid.

tax evasion); or the monies are the product of criminal activity (e.g., smuggling and trafficking in minerals, wildlife, drugs, and people); or the money is being utilized for nefarious reasons (e.g., financing of organized crime).<sup>29</sup> For the purposes of this study, overall, IFF can be seen as those cross-border economic transactions which aim at illegal activities or assisting non-legitimate groups, which may threaten humankind via generating unlawful activities.

### 3. Relationship between IFF and Regulatory Framework

The introduction of the term “IFF” happened in the early 90s by international organizations to address a development challenge of developing countries (OECD, 2016).<sup>30</sup> The leading organizations have agreed that because IFF, from developing countries to developed countries, hinders the sustainable development goals. Certainly, the weakened legal structure of the national institutions remains the key provoking mechanism of IFF for the developing nations, since IFF covers a large part of policy areas with small loops.<sup>31</sup> Subsequently, combating IFF remains a concerning matter for policymakers of all time and the institutional framework.

The proper implementation of those strong policies by government stakeholders through establishing an anticorruption environment can enable fighting against IFF at all levels. In line with this view, Dohlman and Neylan (2020) have stated five major interlinked policy areas that can control IFF at any national level, which include criminal justice, regulation and supervision of financial institutions and professions, the tax system, government and public administration, and company and trust law.<sup>32</sup>

Following the objective of this study, the relationship between IFF and the regulation and supervision of financial institutions and professions has been considered in this part. At the same time, with regard to controlling illicit finance, scholarly emphasis has been on the sensible regulation of the financial institutions and their business models along with consumer behavior as well as data protection. For instance, Dohlman and Neylan (2020, 20-21) believed that,

*As well as preventive measures to counter illicit finance, financial institutions are also subject to prudential supervision, and supervision of their conduct of business, consumer protection, and data protection. These different supervisory regimes have*

<sup>29</sup> WB, “Illicit Financial Flows (IFFs),” The World Bank, <https://www.worldbank.org/en/topic/financialsector/brief/illicit-financial-flows-iffs>.

<sup>30</sup> OECD, “Coherent policies for combatting Illicit Financial Flows,” *Framework for Policy Coherence for Sustainable Development: Thematic Module on Illicit Financial Flows [SG/PCD(2016)3]*, 2016, <http://www.un.org/esa/ffd/ffd-follow-up/inter-agency-task-force.html>.

<sup>31</sup> Ebba Dohlman and Tom Neylan, “Policy Coherence in Combating Illicit Financial Flows: PCSD Thematic Module (2020),” [https://www.oecd.org/gov/pcsd/IFFs%20thematic%20module%20v12c1\\_for%20web.pdf](https://www.oecd.org/gov/pcsd/IFFs%20thematic%20module%20v12c1_for%20web.pdf).

<sup>32</sup> Ibid.

*distinct purposes, different approaches to supervision, and in many cases different agencies are responsible for supervising compliance with regulations relevant to IFFs and for other forms of financial supervision. A consistent approach to these various regulatory regimes and their supervision is desirable to enable a coherent compliance culture in financial institutions (for example with a consistent approach to risk, so that managers do not face a zero-failure regime on one issue, and a risk-based approach on another), and to avoid overburdening the financial sector and their supervisors. It can also enable synergies between different 21 forms of supervision, e.g., where there are red-flag indicators of IFF activity which are visible to a prudential supervisor, but not normally reviewed by AML/CFT or conduct or business supervisors.<sup>33</sup>*

According to Dohlman and Neylan (2020), these regulations should have a wider scope with different approaches in different areas, sometimes the form of supervision and the implementation agencies can be different, thus can create a filtering net against illicit finance and procuring financial agencies.<sup>34</sup> In continuation, Dohlman and Neylan (2020) have further highlighted who would be the responsible authority to supervise financial organizations. Beyond the border, cooperation of monetary regulatory authorities via promoting financial sector standards and links between the standard-setters like the Financial Stability Board (FSB), the Basel Committee on Banking Supervision (BCBS); the International Organization of Securities Commissions being an association of organizations (IOSCO); and the International Association of Insurance Supervisors (IAIS) can regulate IFF.<sup>35</sup> At the border, the responsible authority for supervision may have a single body divided into several organs or have a network of separate supervisors for each sector, including banking, insurance, securities sectors, and regulated businesses and professions.<sup>36</sup> However, the standards may vary from country to country.

#### **4. Logical Structure of the Regulatory Framework**

From the local to global, the regulation remains an important part of optimal policy making both in the public and private spheres. With the beginning of the fourth generation of industrialization (Industry 4.0), the actions of regulatory frameworks become more complex since the actors both in public and private sectors have to deal with individual behavior at global, national, and local levels on the same platform. Whereas traditionally ‘how to regulate in better ways’ remains an important part of governmental agencies, nowadays understanding a better approach to regulation has become a multidisciplinary concern. In any

---

<sup>33</sup> Ibid.

<sup>34</sup> Ibid.

<sup>35</sup> Ibid.

<sup>36</sup> Ibid.

case, ‘building better’ has always been a major concern of policymakers, and remains a formal step for different actors. From this point of view, Bluff (2018) has identified five different regulation theories (Table 1) which are generally practiced all over the world. In this section of this study, it is important to understand which theory will best fit for explaining Bangladesh’s existing online regulatory frameworks and which theory can help to move this structure one step ahead.<sup>37</sup>

**Table 1: Five different regulation theories<sup>38</sup>**

	<b>Theories</b>	<b>Description</b>	<b>Example</b>
1.	The Risk-based regulation	Based on an assessment of threats to the regulator's objectives, the regulator employs systematized decision making to prioritize regulatory actions and deploy resources.	food safety policy in different countries
2.	The Regulatory craft	Regulators examine specific problems, threats, or risk concentrations in a systematic manner and respond with specific interventions or solutions.	The Australian Skills Quality Authority (ASQA)
3.	The Responsive regulation	Aims to balance cooperative and deterrent regulatory tactics by using a pyramid of supports to gradually increase regulator capacity and reinforce strengths, and if that fails, a pyramid of progressively more punitive punishments is implemented until reform is achieved.	Work place Safety and Insurance Board (WSIB) in Ontario Canada
4.	The Smart regulation	Builds on responsive regulation by implementing a three-sided pyramid in which government, business, and third-party regulators all work together to implement complementing mechanisms in a coordinated manner.	The Dutch Inspectorate of Environment in the Netherlands
5.	The Strategic enforcement	Supply chains, branding, franchising, third-party management, and other business systems are used by regulators to design and target interventions.	The Working Hour Division (WHD) of the Department of Labor in the United States

<sup>37</sup> Elizabeth Bluff, “Regulatory Theories and Frameworks,” in *Hybrid Public Policy Innovations*, eds. Mark Fabian and Robert Breunig (New York: Routledge, 2018), 46–62.

<sup>38</sup> *Ibid.*



In implementation the above-mentioned five theories have their effectiveness on their subject matter. To discuss this, Bluff (2018, 58) has further mentioned,

*In risk-based regulation the regulatory response is proportionate to risk, while in responsive and smart regulation the regulator is responsive to reform (or not) by regulates. The regulatory craft and strategic enforcement are more concerned with regulator tactics; that is, planning strategies or actions to achieve a specific end. In risk-based regulation the priorities for attention are the risks or regulates that pose the likeliest threat to the regulator's objectives. By contrast, the regulatory craft calls for assessment of identified harms to determine priorities. The approach of strategic enforcement is different again as it prioritizes influential actors in supply chains and business systems that give rise to systemic non-compliance. Responsive and smart regulation shed little light on priority setting.<sup>39</sup>*

Apart from Bluff's (2018) perceptions, UNODC and OECD (2016, 5) have recommended four coherent frameworks to combat IFF, which include "identifying and raising awareness of the types, magnitudes, and risks of IFFs (particularly at the political and policy-making level); considering the contextual factors that allow IFFs to thrive; supporting coherence within and between national and international normative frameworks (vertical coherence); Identifying critical, prioritized interactions across economic, social and environmental areas to address IFFs (horizontal coherence)".<sup>40</sup> In this study, the presented theories will be used to explain the nature of Bangladesh's e-commerce regulatory framework and which one could be better to minimize the IFF through e-commerce.

## 5. Study Design

A comparative research method applying a qualitative approach has been adopted to assess the effectiveness of the existing Bangladeshi digital commerce regulatory framework to reduce IFF. The whole research has been structured in three parts. The study questions and objectives have been presented in the introduction, as well as the parameters of comparative analysis and the relevant assessment criteria. The second section has examined developing mechanisms and instruments and considers their impact on the national financial flow equilibrium. Lastly, the conclusion has been drawn along with recommendations for strengthening the subject's regulatory

---

<sup>39</sup> Ibid.

<sup>40</sup> OECD, "Coherent Policies for Combatting Illicit Financial Flows," *Framework for Policy Coherence for Sustainable Development: Thematic Module on Illicit Financial Flows [SG/PCD(2016)3]*, 2016, <http://www.un.org/esa/ffd/ffd-follow-up/inter-agency-task-force.html>.

mechanisms to combat the pressure of emerging platforms and to secure the national economy.

Several secondary sources like different countries as well as organizations' policies were the primary source of data. Through contentment analysis, the comparative discussion has presented under some themes like contractual information, payment gateway, withdrawal period, use of cookies, data protection, notification of purchase, VAT rules, cross-border delivery rules, customs and taxation rules, online banking rules, and so on. Later based on these findings the researcher has to seek the answer to the second research question as to how illicit financial flow via digital platforms can be minimized through an effective policy measure in Bangladesh with reference to different successful policy initiatives in other countries or regions.

## **6. Brief Economic Background of Bangladesh and Its E-commerce Legal Framework**

Bangladesh is the fastest developing country in South Asia. By the Fiscal Year (FY) 2020-2021, the GDP growth rate was 5.47 percent, and it was 8.15 percent in FY 2018-19. In comparison to the previous fiscal year, per capita, the national income was USD 2,227, up from USD 2,024 before. In FY 2020-21, the budget deficit is expected to be approximately 6.1 percent of GDP. Therefore, to improve tax administration transparency, steps have been taken to further automate and digitize the income tax (IT), value-added tax (VAT), and customs agencies. A value-added tax system based online has already been implemented. The execution of current reform programs is projected to aid in keeping the budget deficit under the 5% limit in the following years. Importantly, the remittances inflows for FY 2020-21 totaled US\$ 24.78 billion, increasing by 36.10 percent from the previous fiscal year.<sup>41</sup>

However, Bangladesh has a lag of a unified legal framework to regulate the rights of consumers and sellers in relation to online trade and commerce. The existing commercial legal structure consisted of the Contract Act of 1872, the Sale of Goods Act of 1930, the Consumer's Right Protection Act 2009, and the Competition Act of 2012, which need to be reshaped according to various aspects of e-commerce. The current Bangladeshi digital sector is generally governed by the ICT division of the Government of the People's Republic of Bangladesh. Under this ministerial division, Bangladesh has taken different digital policies to regulate online business and other activities. For instance, the Digital Commerce Operation Guidelines 2021, National ICT Policy 2018, National Digital Commerce Policy 2018, Government e-Mail Policy, Digital Bangladesh Award Policy 2021, National ICT Policy 2009, National ICT Policy

---

<sup>41</sup> BER, "Bangladesh economic review 2021," in Dhaka: Ministry of Finance, Government of the People's Republic of Bangladesh, 2021, <https://mof.portal.gov.bd/site/page/28ba57f5-59ff-4426-970abf014242179e/Bangladesh-Economic-Review-2021>.

2015, Policy for fellowship, scholarship, and grants for research and innovation in the ICT sector – 2016, Digital Security Rules-2020, National Strategy for Robotics, National Blockchain Strategy: Bangladesh, User’s Policy for National Data Center, Bangladesh Computer Council, User’s Policy for National Data Center, Bangladesh Computer Council. Nevertheless, by 2021 several e-commerce fraud and scam cases had come to light and revealed the weakness of the existing policy, which is susceptible to provoke IFF. However, to overcome the challenge, recently the Ministry of Commerce (MOC) of the Peoples Republic of Bangladesh has issued some standards and rules applicable to e-commerce operators known as the Digital Commerce Operational Guidelines 2021 (“the Guidelines”), but still, it remains a question of legal bindings.

Howsoever, the Ministry of Commerce is the sole authority to regulate Bangladesh’s national as well as foreign trade and commerce under the Competition Act, 2012. The objectives of this government stakeholder are to ensure a sound competitive market environment through creating a business-friendly environment, price stability for essential commodities through adequate supply, enhanced market access for Bangladeshi exports, and protection of rights and interests of consumers. On the one hand, the Committees on Consumers’ Right Protection have monitored consumer rights in 64 districts. On the other hand, the Business Promotion Council is responsible for introducing and implementing an appropriate program for export diversification. To keep pace with the changing nature of global trade and commerce the ministry, following a risk-based regulatory framework, has adopted a new policy, namely, the Digital Commerce Operation Guidelines 2021 (original in Bengali) of Bangladesh, which is governed by the Digital Security Act, 2018 (Act No. XLVI of 2018) of Bangladesh. In the following discussion, the author will present a brief overview of this latest policy and act, which are the soul of Bangladeshi e-commerce.

## **6.1 Digital Commerce Operation Guidelines 2021**

The latest Digital Commerce Operation Guidelines 2021 of Bangladesh (original in Bengali) is the modified version of the Digital Commerce Operation Guidelines 2020 (the amended version of the National Digital Commerce Policy, 2018) aiming to provide transparency and accountability in the digital commerce industry, creation of employment opportunity, protecting consumer rights, and growing dependence on digital commerce by establishing a regulatory framework, and fostering a competitive market with possibilities for entrepreneurs.<sup>42</sup> Unlike the previous one, the guideline has defined the Marketplace and its rules to regulate. According to the policy, a marketplace is

---

<sup>42</sup> Law Desk, “An overview of the Digital Commerce Operation Guidelines 2021,” *The Daily Star*, 2021, <https://www.thedailystar.net/law-our-rights/news/overview-the-digital-commerce-operation-guidelines-2021-2128871>. The People’s Republic of Bangladesh, “Digital Commerce Operation Guidelines 2021,” Dhaka: The People’s Republic of Bangladesh, Ministry of Commerce (2021).

a digital commerce site that provides information on goods and services offered by one or more third parties, as well as facilitates transactions. And as a basic rule, the Guideline says unless otherwise agreed between them, the marketplace is obligated to pay the third-party vendor within 10 days after deducting relevant charges/commissions.<sup>43</sup>

Moreover, this Guideline applies to all organizations that are conducting business within the country. Thereafter, certain regulations have been postulated in this guide which should be followed by all business organizations. For instance, the necessity to specify the specific terms of purchase and return, to indicate the number of products, their ingredients, price, shipping or other costs, and to give an image, video, or other representation of the items to be sold for the buyer to make an educated decision. Side by side, certain restrictions on digital commerce platforms are also addressed in this policy which include that no addictive or illegal material may be sold; no arrangement for online betting or online gambling may be formed; and no lottery or raffle draw may be held in violation of the Penal Code, 1860, and without the approval of Bangladesh Bank. Besides, without a license from the Directorate General of Drug Administration, no digital commerce site can offer pharmaceuticals or health care products.<sup>44</sup>

For data protection, this policy has highlighted, that to get any personal data, digital commerce platforms must first obtain the buyer's consent by explaining why the data is being collected, where it will be stored, how it will be processed, and for what reasons it will be used. A “check-box” on the website can be good for this. Apart from these, all business-related information must be kept for at least six years and made available to any government entity upon request. Without the consent of Bangladesh Bank (where applicable) or in violation of Bangladesh Bank's instructions, no digital wallet, gift card, cash voucher, or other alternative payment methods may be implemented. The delivery timeline has also been clarified: products sent within the same city should be delivered within 5 days provided payment is received, while products shipped to a different location should be delivered within 10 days, according to the Guideline. For commodities that are used frequently or are perishable, delivery must be expedited, and the customer must be informed of this.<sup>45</sup>

For the complaint and redress mechanisms, some guidelines have been set for the Marketplaces, such as, consumers must have access to a phone number, email address, or other means of contact to make a complaint. Such concerns must be documented, and the consumer must be given a remedy within 72 hours. Digital commerce platforms must also guarantee that an appropriate rating and review system is in place so that purchasers can see them and make an educated decision, and that such reviews cannot be removed by the platform. The authority may take required actions or file a complaint with the appropriate

---

<sup>43</sup> The People's Republic of Bangladesh, “Digital Commerce Operation Guidelines 2021”.

<sup>44</sup> Ibid.

<sup>45</sup> Ibid.

government agencies against any platform that does not follow the Guidelines - these actions include the termination of a trading license, business registration, VAT registration, and so on. Buyers can also file a complaint with the Directorate of Consumer Rights Protection for compensation for any losses incurred as a consequence of noncompliance. Furthermore, it is also required to have a Unique Business Identification Number (UBID) for each organization in the marketplace. All international digital commerce platforms that conduct business in Bangladesh must register in Bangladesh and receive the appropriate approvals from the relevant authorities, according to the rules.<sup>46</sup>

Though this latest digital commerce guideline 2021 has created a space for the direct inspection of the government, in some area criticisms have been raised. For instance, Chomok and Roni (2021) have stated “although the guidelines provide instructions for complaints, it fails to mention detailed instructions and procedures following a complaint by a customer”. Besides the complaint issue, to resolve some issues these Guidelines depend on the Consumer Rights Protection Act, 2009 (CRPA) but CRPA does not cover all those issues which have not been highlighted in this latest one. For example, CRPA does not apply to online transactions, which is a major loophole of this guideline, provoking IFF.<sup>47</sup>

Criticizing the policy, Chomok and Roni (2021) further highlighted that very few specific instructions have been given to minimize the excessive discount or predatory pricing, which have been weaponized by the Evaly and Alesha Mart to do their fraud activities against consumers.<sup>48</sup> Here, e-commerce organizations like Evaly and Alesha Mart have offered predatory prices with luring cashback offers, which motivated customers to wait for 3-4 months to get their goods or services, and in the meantime, these organizations have withdrawn their business.<sup>49</sup> Apart from these, no guidelines can be found on the cross-border e-commerce legislative issue. Having these weaknesses, the possibility to have IFF from Bangladesh has increased.

## 6.2 Digital Security Act, 2018

The Digital Security Act 2018 is the primary legislative instrument in Bangladesh that would apply to the violation of the Bangladesh Digital Commerce Guidelines 2021. This legal instrument defines “Appellate Tribunal” as the Cyber Appellate Tribunal constituted under section 82 of the Information and Communication Technology Act, 2006 (Act No. XXXIX of 2006); “Tribunal” means the Cyber Tribunal constituted under section 68 of the

---

<sup>46</sup> Ibid.

<sup>47</sup> Gargi Das Chomok and Saurov Dash Roni, “Why the new ‘Digital Commerce Operation Guidelines’ needs major revisions?,” *The Daily Star*, 2021, <https://www.thedailystar.net/law-our-rights/law-analysis/news/why-the-new-digitalcommerce-operation-guidelines-needs-major-revisions-2143741>.

<sup>48</sup> Ibid.

<sup>49</sup> Ibid.

Information and Communication Technology Act, 2006 (Act No. XXXIX of 2006); “Criminal Procedure” means the Code of Criminal Procedure, 1898 (Act V of 1898); “defamation” means defamation as defined under section 499 of the Penal Code (Act XLV of 1860)”. As for data storage under this act, all forms of information, knowledge, event, a basic concept, or guideline presented as text, image, audio, or video format, which (i) is being or has been processed by any computer or computer system or computer network formally; and (ii) has been processed for use in any computer or computer system or computer network, have to be taken into account.

Further, a critical information infrastructure in the name of public safety or financial security or public health, national security or national integrity or sovereignty has been included. Here, this section is the key instrument of the law enforcement agency to regulate e-commerce in Bangladesh. This act also clarifies who would be the supervisory stakeholder to apply this Act. According to this legal architecture, such are the Digital Security Agency (under section 5 of this Act); the National Computer Emergency Response Team or Computer Emergency Response Team (under section 9 of this Act); the digital forensic lab (under section 10 of this Act); a police officer who is not below the rank of sub-inspector.

In chapter VI, different levels of punishment related to digital security have been specified. For instance, punishment for illegal access to any critical information infrastructure etc. (section 17); illegal access to computer, digital device, computer system, etc. (section 18); damage to a computer, computer system, etc. (section 19); offence and punishment related to modification of computer source code (section 20); punishment for making any kind of propaganda or campaign against the liberation war, the spirit of the liberation war, the father of the nation, the national anthem or national flag (section 21); digital or electronic forgery (section 22); digital or electronic fraud (section 23); identity fraud or personation (section 24); transmission, publication, etc. of offensive, false or threatening data information (section 25); punishment for unauthorized collection, use etc. of identity information (section 26); offence and punishment for committing cyber terrorism (section 27); publication, broadcast, etc. of information on a website or in any electronic format that offends the religious values or sentiment (section 28); publication, transmission, etc. of defamatory information (section 29); offence and punishment for e-transaction without legal authority (section 30); offence and punishment for deteriorating law and order, etc. (section 31); offence and punishment for breaching secrecy of the Government (section 32); punishment for holding, transferring data-information illegally, etc. (section 33); offence related to hacking and punishment thereof (section 34); abetment of committing an offence and punishment thereof (section 35); offence committed by a company (section 36); power to issue an order for compensation (section 37); non-responsibility of the service provider (section 38).<sup>50</sup>

---

<sup>50</sup> Digital Security Act, 2018 (Act No. XLvi of 2018).

However, in terms of effectiveness to control actual crime, this Act has been criticized severely. For instance, Rahman and Rashid,<sup>51</sup> Ataula and Yildirim,<sup>52</sup> Bari and Dey,<sup>53</sup> Runa,<sup>54</sup> and Azad<sup>55</sup> have criticized the Digital Security Act, 2018, which is also known as the Cyber Security Act, due to the incorporation of some sections, especially sections 25 and 31 of the Act, which are against the right of freedom of speech enshrined in Article 39 of the Constitution of Bangladesh.<sup>56</sup> Besides, this Act has no clear instructions about e-commerce and its regulatory measures. Only, it has highlighted some points in sections 4 and 11 without much explanation or clear punishment for their violation. To combat IFF, there is no clear section presented in this Act, which provokes money laundering.

## 7. Concluding remarks

This study aimed to understand the strengths and weaknesses of the existing e-commerce regulatory framework for minimizing the IFF of Bangladesh. Over the past six years through unknown channels \$49.65 billion was siphoned off from Bangladesh.<sup>57</sup> Most of these currencies are generally earned and distributed by online platforms, which demonstrates the weakness of the legislative structure. Through an intensive review, the author has found that following the risk-based supervisory model the latest e-commerce policy of Bangladesh has guided the digital commerce atmosphere in Bangladesh. To prevent fraud and money laundering issues, the Digital Commerce Guidelines 2021 have clearly stated several issues. For instance, consumer right protection has become a priority and, so, permission to use consumers' personal data has become mandatory. Several indications have also been postulated in this legal framework to ensure a competitive marketplace abolishing monopoly. Illegal

---

<sup>51</sup> Aliur Rahman and Harun Or Rashid, "Digital Security Act and Investigative Journalism in Bangladesh: A Critical Analysis," *CenRaPS Journal of Social Sciences* 2, no. 2 (2020): 216–36.

<sup>52</sup> Muhammed Ataula and Besim Yildirim, "The Digital Security Act 2018 and the Obstacles to Freedom of Speech and Freedom of Media in Bangladesh," *Atatürk İletişim Dergisi* (2021): 69–92.

<sup>53</sup> M. Ehteshamul Bari and Pritam Dey, "The Enactment of Digital Security Laws in Bangladesh: No Place for Dissent," *The George Washington International Law Review* 51 (2019): 595.

<sup>54</sup> Sharmin Jahan Runa, "The Challenges of Freedom of Expression and the Digital Security Act 2018," *BiLD Law Journal* 4, no. 2 (2019): 75–92.

<sup>55</sup> Ananya Azad, "Digital Security Act in Bangladesh: The Death of Dissent and of Freedom of Expression," Central European University, Vienna, 2021.

<sup>56</sup> Republic of Bangladesh, Ministry of Law, Justice and Parliamentary Affairs, 1–24. Dhaka: Government of the People's Republic of Bangladesh, 2018, <http://bdlaws.minlaw.gov.bd/>.

<sup>57</sup> The Financial Express, "\$49.65b Siphoned Off from Bangladesh in Six Years: Gfi," 2021, <https://thefinancialexpress.com.bd/public/index.php/trade/4965b-siphoned-off-from-bangladesh-in-six-years-gfi-1639797327>.

products, gambling, and lottery have been prohibited in these guidelines. So, such major issues have been addressed clearly, which is likely to have an impact on money laundering. But still, several fraud cases related to online business have been experienced by the local consumers of Bangladesh. How has it happened?

The findings of this study show that neither the Digital Commerce Guidelines, 2021 nor the Digital Security Act, 2018 has postulated any specific definition of online transactions. Subsequently, provocation of IFF becomes so easy. Lack of detailed instructions and mode of complaint by a customer has also helped organizations like Evaly and others to commit fraud. The lack of legal provisions on the supervision of excessive discounts or predatory pricing has been found as another weakness of the existing regulatory framework of Bangladesh. Lastly, no standards or guidelines for cross-border e-commerce have been placed in the existing legal supervisory structure. Thus, it is recommended to rethink these weaknesses of the latest policy to reduce IFF.

Further, it is also recommended to follow the Strategic Enforcement method to regulate this constantly changing and diversified marketplace. Through this method, a regulatory body can constantly supervise supply chains, branding, franchising, third-party management, and other business systems. Nevertheless, the current policy follows the traditional supervisory model where actions are taken only after a threat has been identified. Based on these recommendations the policymakers can rethink the core structure of the existing regulatory framework in Bangladesh to minimize IFF.