

الدراسة الثانية:
العملات المشفرة في لبنان بين
الواقع والتشريع
**Cryptocurrencies in Lebanon between reality
and legislation**

د. زهير رشاش بشناق

Cryptocurrencies have gained increasing interest due to their reliance on Blockchain technology, which has proven to be a promising future. After the year 2009, it moved from just the idea to the actual application on the ground with its founder, Satoshi Nakamoto. There are thousands of active digital currencies around the world (about 1,423 coins on one platform) with a market value of \$1.3 trillion. Hundreds of currencies, the most important of which are Luna and Tera, died recently on May 17, 2022 due to their inability to continue in the market, and Bitcoin acquired the lion's share of them.

The cryptocurrency Bitcoin was launched in 2009 and is the first currency in terms of widespread access. Thousands of investors in trading operations have succeeded in earning millions thanks to their early demand for investments in Bitcoin, as is the case in most other digital currencies where investors attract this experience and try to reproduce it.

The fluctuations of currency rates according to the rise and fall of the markets, and what the currency rates witnessed recently, and the lack of steadfastness and collapse of some have sparked a great controversy about its regulation. Cryptocurrency mining is also very costly in terms of energy and pollution, and digital currencies globally generate a huge amount of carbon dioxide. Bitcoin, for example, which is the most popular cryptocurrency, produces as much carbon dioxide as New Zealand.

Despite the volatility of the market, Bitcoin continues to be in trading, mainly due to the increasing number of investments in the areas of blockchain gaming and the efforts made by the virtual world technology Metaverse.

But encrypted digital currencies are both a target and a criminal tool for criminals, as they devise daily modern means and methods to implement their schemes that deal with virtual digital currencies. While the absence of regulatory and punitive legislation contributes to their evasion of criminal prosecution and punishment. In this case, the aggrieved person stands without legal protection and

the absence of any means to return his looted money or his lost rights. Some experts believe that bitcoin and virtual currencies have unleashed electronic black markets, as organized crime, economic and financial have become more complex in the past years.

Cybercrime is committed by individuals or organizations, and some of these cybercriminals are organized and use advanced technologies and the black internet and are highly technical, and some are just novice hackers.

Modern types of cybercrime include, or at least one of the following, criminal activity that targets computers using viruses and other types of malware, and criminal activity that uses computers to commit other crimes. Research has shown that about a third of the world's population can understand the data and statistics that constitute the only output of the open data movement

. But blockchain technology goes much further than that as it requires citizens to accept a new approach to data management and to have some understanding of encryption and key management principles or face losing their money or government services, and this needs knowledge and knowledge that can only be done according to a plan in the medium and long term. Hence the call for international solidarity and direct solutions to the serious impact of crimes committed in one country on the interests of individuals and bodies in other countries

It is necessary to set up a legislative workshop, focus on education, the youth category, support emerging institutions, and take into account the reform of the protective digital laws, because civil and penal service workers, judges and judicial officers in prosecution offices should be more than just conversant with technology. Accordingly, we suggest the following recommendations, which are valid for all countries:

1- Creating an innovation environment for legal uses of modern technologies and spreading awareness of its importance and how to protect it and introduce it into the curriculum and from the primary grades, and the need to realize the importance of education for all and how to manage the data highways on which our society is built now and in the future.

2- Adopting the digital identity, enhancing reliability and the protection network to allow individuals and small and medium-sized companies to access the services they need, and strengthening artificial intelligence techniques that are used in auditing and control.

3- Issuance of a framework law regulating platforms and conditions for issuing encrypted electronic and virtual money and mining operations, and setting good faith principles for trading in cryptocurrencies

4- Establishing and supporting the "National Agency for Security and Information Systems" in accordance with the National Cyber Security Strategy. Protection includes government departments, e-commerce, companies and individuals from cyber-attack, all forms of piracy, content tampering, terrorism,

regulation and supervision to manage the risks of these modern technologies more effectively with the aim of providing a safe work environment that facilitates cooperation and data sharing in close cooperation with authorized, legal and controlled service providers and checking.

5- Establishing a flexible criminal law for cybercrime as a framework law and the adoption of decrees and mobile systems, in which international jurisprudence can be relied on, and the courts may rely on the case decided in cyberspace, which can keep pace with new developments.

6- Establishing a Public Prosecution and a specialized criminal court on the Internet that follows the judicial system and that every person or entity around the world can sue over the Internet while respecting the established rules of private international law, and it has the rules of its trials, provided that the police body that undertakes prosecution and coordination internationally through Interpol is strengthened.

7- Establishing a chamber in a virtual commercial court to deal with smart contract disputes. The codification of social norms in smart contracts cannot be left to be handled only by startups or by young money aspirants because the way it is implemented has an impact on a large number of people and therefore needs to be managed across society. A coded contract written in one country under a certain set of laws has an effect on the citizens of another country.

8- Establishing open judicial rooms specialized in the Internet, linked to the Arab Ministries of Justice, Education and Higher Education, and linking them to the pages of all Arab universities, exchanging opinions and experiences, receiving complaints and developing solutions to enhance the legal culture of students to be informed of all new systems, emerging crimes and their penalties, the danger of adopting the black network, enhancing financial awareness and the importance of personal data And respect for privacy in the Internet space.

○ مقدمة

اكتسبت العملات الرقمية المشفرة إهتماماً متزايداً لاعتمادها على تقنية البلوكتشين Blockchain Technology والتي اثبتت أنها المستقبل الواعد، وانتقلت بعد العام ٢٠٠٩ من مجرد الفكرة إلى التطبيق الفعلي على أرض الواقع مع مؤسسها ساتوشي ناكاموتو^(١). ويوجد ألوف العملات الرقمية الفاعلة حول العالم (حوالي ١٤٢٣ عملة على منصة واحدة) بقيمة سوقية تبلغ ١.٣ تريليون دولار. وماتت مئات العملات وأهمها لونا وتيرا مؤخراً في ١٧ أيار ٢٠٢٢ لعدم قدرتها على الاستمرار في السوق، واستحوذت عملة بتكوين (Bitcoin) على حصة الأسد منها^(٢). وبدأت عملة البيتكوين المشفرة في عام ٢٠٠٩ وهي العملة الأولى من حيث الوصول إليها على نطاق واسع. وقد نجح الآلاف من المستثمرين في عمليات التداول من كسب

(1) Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", 2008
www.bitcoin.org/bitcoin.pdf

(2) <https://dappradar.com/hub/tokens/ethereum/all/57>

الملايين بفضل إقبالهم على الاستثمارات في عملة البيتكوين في وقت مبكر، وكذلك الحال في معظم العملات الرقمية الأخرى حيث يجذب المستثمرون هذه التجربة ويحاولون استنساخها. إن تقلبات أسعار العملات بحسب ارتفاع الاسواق ثم انخفاضها وما شهدته أسعار العملات مؤخراً، وعدم صمود وانهيار البعض قد أثار جدلاً كبيراً حول تنظيمها. كما أن تعدين العملات المشفرة الرقمية باهظ الكلفة على صعيدي الطاقة والتلوث، وتتسبب العملات الرقمية عالمياً بتوليد كمية هائلة من ثاني أكسيد الكربون. تنتج عملة بيتكوين مثلاً وهي الأكثر شعبية بين العملات الرقمية المشفرة كمية من ثاني أكسيد الكربون تضاهي ما تنتجه نيوزيلندا.

ولا يزال وضع عملة البيتكوين في التعاملات مستمرة رغم التقلبات التي مر بها السوق، ويرجع هذا بشكل أساسي إلى العدد المتزايد في الاستثمارات في مجالات ألعاب البلوكتشين والجهود المبذولة من تقنية العالم الافتراضي الميتافيرس. وبحسب أحدث الإحصائيات المستمدة من خدمة تحليلات شركة دابرادار (dapradar)، فقد أثبتت ألعاب البلوكتشين صدارتها كونها الفائز الفعلي طوال فترة ركود العملات الرقمية⁽¹⁾. فقد حققت ألعاب البلوكتشين نمواً بواقع ١٠ % منذ الربع الأول من العام ٢٠٢٢، حيث احتلت ألعاب البلوكتشين موضعها كصناعة رئيسية بفضل أدائها الأقوى خلال فترة جائحة كورونا والتداعي والركود التي شهدتها الأسواق حول العالم⁽²⁾.

تتوفر العملات المشفرة على الشبكة، ويقوم المستخدم بشرائها من خلال الشركات المختصة ببيع العملات الافتراضية، حيث يتم إنشاء عنوان خاص به أو رقم خاص بالمحفظة الإلكترونية التي يخزن العملات ضمنها، ويعتبر هذا العنوان الوسيلة الوحيدة للمستخدم التي تسمح له بالتداول بالعملات الافتراضية عبر الإنترنت.

تعمل البيتكوين وسائر العملات المشفرة بشكلٍ مستقل عن أي مصرف أو دولة، وليست بحاجة لبنوك مركزية لإصدارها وتعتمد على تقنية البلوكتشين، وهي عبارة عن سجل عام موزع Distributed Ledger، تسمح بتسجيل البيانات ونقلها على الشبكة مستندة إلى تقنية التشفير Cryptography. وقد تكون البديل عن تدخل المصارف المركزية ودورها في إصدار العملات، وتحديد دورها في الاقتصادات الوطنية والسياسة المالية⁽³⁾. ويتم تخزين العملات الرقمية في محافظ رقمية خاصة، وهي عبارة عن برامج أو تطبيقات يتم تثبيتها بواسطة المستخدمين على أجهزة الكمبيوتر أو الأجهزة المحمولة الخاصة بهم. وتحتوي كل محفظة رقمية على معلومات مشفرة، تسمى المفاتيح العامة والخاصة، والتي تُستخدم لإرسال العملة الرقمية واستلامها. يتم تسجيل جميع معاملات العملة الرقمية في سجل أساسي عام أو دفتر أستاذ عام افتراضي

(1) <https://dapradar.com/hub/tokens/ethereum/all/1>

(2) https://www.albayan.ae/economy/uae/2022-10-01-1.4526805?itm_source=parsely-

(3) Grégory Claeys, Maria Demertzis and Konstantinos Efstathiou, "Cryptocurrencies and monetary policy", ECON Committee of the European Parliament, 2018

يسمى بلوكتشين، والذي يتم حمايته وحفظه بواسطة عمال تعدين العملة الرقمية. المعدنون او عمال التعدين يتواجدون في أي مكان في العالم، ويملكون أجهزة كمبيوتر متخصصة لمعالجة العمليات الحسابية المعقدة بسرعة. ويستفيد عمال التعدين من عملات رقمية، مثل Bitcoin و Ripple و Dogecoin و Litecoin ، مقابل التحقق من كل معاملة وإضافتها إلى البلوكتشين.

هذه المواقع في الغالب هي مواقع غير رسمية، ويتم إنشاؤها من قبل أشخاص يتمتعون بخبرات عالية في المجال التقني والمالي والقانوني والدعائي، ويحمون أنفسهم من الملاحقة القانونية، فالقواعد القانونية العامة لا تسعف المستخدم أو السلطات المختصة من ملاحقة مصدري العملات الافتراضية أو المواقع الوهمية^(١). وفي قضية إحتيال وسرقة العملات الرقمية كانت الاولى من نوعها في الامارات العربية تمت سرقة ٢٥ بيتكوين عبر تحويلها من حساب الى حساب بالقوة وقد وصلت هذه القضية الى خواتيمها وتم تجريم الفاعلين بجرم الخطف^(٢).

تعتبر العملات الرقمية أو الافتراضية وسيلة للتبادل في الولايات المتحدة ولكن ليس لها قوة ابرائية كالنقود العادية مثل الدولار والعملات المعدنية، ولا يتم إصدار العملات المشفرة أو دعمها من قبل حكومة الولايات المتحدة، ولكنها محط انتباه وتركيز كل الولايات حاليا. فالجميع لديهم تقدير بأن تقنية بلوكتشين هي المستقبل ويجب ان يتم تنظيمها على مستوى الولايات جميعا^(٣). ويرى آخرون ان العالم اليوم في لحظة فريدة من نوعها في التاريخ حيث يمر المجتمع بمرحلة انتقالية من الاقتصاد الصناعي إلى الاقتصاد الذي تحدده مجموعة جديدة من التقنيات، تتراوح من التكنولوجيا الرقمية إلى التكنولوجيا متناهية الدقة. وتبرز تقنية البلوكتشين من بين أحدث موجات الرقمنة، وهي تقنية يقول الكثيرون إنها تعد بإعادة تعريف الثقة والشفافية والضمان في جميع أنحاء العالم. ومع ذلك، يعتبر بعض المفكرين تقنية البلوكتشين غير ناضجة نسبياً ويمكن أن تخلق العديد من المشكلات بقدر الحلول التي توفرها^(٤). ولم تحظر معظم الولايات البتكوين وغيرها من العملات المشفرة واعتبرتها شكل من أشكال العملات الرقمية المستخدمة في معاملات الدفع الإلكترونية، لسهولة ويسر التعامل بها دون استخدام العملات المعدنية أو النقود الورقية، ويتداول بها المستخدمون في الواقع دون المرور بالبنوك، وبحد أدنى من رسوم التعاملات، وذلك نظرا لتأمين تعاملات سريعة وغير مرتبطة بالجغرافيا، وإبقاء التعاملات سرية ومجهولة المصدر. وتتجه معظم الولايات الى

^(١) عبد الله ناصر عبيد نصيري الزعابي، رسالة ماجستير، جامعة الامارات ٢٠١٨

A Critical Analysis on Legal Regulation of Digital Currencies Newly Included in UAE and Comparative Legislation

^(٢) <https://www.albayan.ae/across-the-uae/accidents/2018-11-26-1.3419218>

^(٣) Joe Dewey, blockchain and cryptocurrency laws and regulations, Hollannd&knight LLP, 21/10/2021

موجود على الموقع

<https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/usa>

^(٤) كاثي موليجان، تقنية سلسلة الكتل "البلوك تشين" والنمو المستدام، تشرين أول ٢٠٢٢. موجود على الموقع <https://www.un.org/ar/44863>

التشريع والاعتراف بأهمية التقنية بتحفّظ، حيث تناولت ٣٧ ولاية تشريعات متعلقة بالعملات المشفرة والعملات الرقمية أو الافتراضية والأصول الرقمية الأخرى في الجلسة التشريعية لعام ٢٠٢٢^(١).

وعلى صعيد الموقف الاوروبي والدولي هناك تباين في مواقف الدول والمنظمات الدولية حول قانونية تداول العملات المشفرة وانقسمت الاراء بهذا الشأن إلى ثلاثة: الرأي الأول جرم تداول العملات الرقمية الافتراضية واعتبرها مضاربة لتحقيق أرباح وتؤثر على النقد والاقتصاد الوطني. أما الرأي الثاني فشرع التداول بالعملات الرقمية المشفرة ومنها السلفادور والصين والتي تراجعت عن تداولها بعد الآثار السلبية التي واجهتها. أما الرأي الثالث فقد حذر من التداول بالعملات الرقمية المشفرة للمخاطر المالية التي قد يتعرض لها المتعاملين بها ومنها لبنان وتتوفر في هذه الدول صياغة أو مؤسسات مالية تقبل بتحويل العملات الرقمية الافتراضية إلى عملات أخرى معتمدين على ضعف الرقابة وعدم وضوح العقوبة.

وسبق أن حذر مصرف لبنان عام ٢٠١٤ من استخدام العملات الرقمية والذي وصفه بأنه مضاربة. ثم أصدر حاكم مصرف لبنان بصفته رئيس هيئة الأسواق المالية عام ٢٠١٨ حظراً على المؤسسات المالية المرخصة على إصدار نقودا إلكترونية ومنع تسويق العملات الرقمية أو التداول بها، لحسابها أو لحساب عملائها، بصورة مباشرة أو غير مباشرة، بما فيها المتداولة في الأسواق المالية المنظمة. في حين حذر الجمهور من شراء العملات الرقمية ومنها البتكوين والتداول بها بكونها تشكل وسيلة هامة للمجرمين.

وتعمل الامم المتحدة على وضع استراتيجية تواكب تقنية البلوكتشين والعملات المشفرة لتوحيد الجهود من خلال إيجاد حلول مناسبة متعددة الأطراف حيث يمكن معالجة التقنيات الناشئة الحالية ووضع أطر مرجعية معقولة لتلك التي لم يتم التفكير فيها حتى الآن. وتبرز أهمية التعامل مع التقنيات الجديدة في وضع استراتيجية الأمين العام بشأن التقنيات الجديدة لعام ٢٠١٩، ودراسة متأنية للتقنيات والعملات المشفرة والعمل

^(١) Heather Morton Cryptocurrency 2022 Legislation 6/7/2022

تقرير على موقع المؤتمر الوطني للمشرعين في الولايات المتحدة
<https://www.ncsl.org/research/financial-services-and-commerce/cryptocurrency-2022-legislation.aspx>
من أمثلة التشريعات التي تناولت العملات المشفرة عام ٢٠٢٢ ما يلي:
طلبت ولاية كونيتيكت من مجلس أمناء التعليم العالي تطوير برامج الندوات لمساعدة الشركات الصغيرة على التكيف مع بيئة الأعمال في أعقاب جائحة COVID-19 من خلال دورات في المجالات الدراسية، بما في ذلك، على سبيل المثال لا الحصر، التجارة الإلكترونية ووسائل التواصل الاجتماعي والأمن السيبراني والعملة المشفرة الافتراضية.
وسنت ولاية إنديانا تشريعاً يضيف فصلاً جديداً إلى القانون التجاري الموحد (UCC) الذي يحكم التعاملات التي تتطوي على سجلات إلكترونية يمكن التحكم فيها.
طلبت ولاية ساوث داكوتا من المرخص له بإطلاق عملات افتراضية أن يحتفظ بعملات افتراضية من نفس النوع ومن نفس الحجم ضمن الترخيص.

قامت ولاية واشنطن وفيرجينيا الغربية بتحديث قوانين الملكية المتروكة والتي لم يطالب بها أحد لتشمل العملات الافتراضية. عدلت ولاية وايومنغ الأحكام القانونية التي تنظم المنظمات المستقلة اللامركزية التي تتعاطى العملات المشفرة وسمحت بشراء تذاكر البانصيب بعملة افتراضية. وفرضت على الكيانات التجارية التي تشارك في خدمات حفظ الأصول الرقمية دفع ضريبة، وسمح لأمين خزانة الولاية بإصدار الرموز المميزة الثابتة وإنشاء لجنة رقابة على ان تكون المراقبة والتدقيق المستقل.

معاً لتقييم تأثيرها والتعامل معها^(١). وجذبت تقنية البلوكتشين اهتمام الناس حول العالم لأنها وجدت أهمية خاصة بالمشاركة في صنع القرار والاستثمار والابداع والتجارة وتعزيز الثقة والتعددية عبر الانفتاح مباشرة على العالم دون المرور بالحوجز التقليدية للدول. هذا التعاون المشترك بين الناس أوجدته تقنية البلوكتشين من منظور خاص. ويرى خبراء أنها رسالة دعوة للتعاون والانفتاح الدولي ونقاش كل المشاكل في العالم والعمل سوياً على ابتكار الحلول، وستستمر لعقود عديدة قادمة ويجب إيجاد طرقاً جديدة للاستجابة عبر الحكومات والمجتمع المدني والأوساط الأكاديمية والمنظمات غير الحكومية والمنظمات الدولية مثل الأمم المتحدة. إن الإيجابية الرئيسية لتقنية البلوكتشين أظهرت حلولاً جديدة تماماً للمشاكل القديمة عندما تم تسليم طاقة الحوسبة إلى قسم كبير من الناس حول العالم بدلاً من الاحتفاظ بها فقط في الشركات، وخلقت تقنية البلوكتشين شكلاً جديداً من النظام المصرفي، وأصبح النظام المنافس في العالم الرقمي الذي بدأنا جميعاً بالعيش فيه. لقد تم بالفعل إطلاق مفهوم الحلول التي تقودها الناس والمملوكة من الناس لكل المشاكل العالمية سواء عالجت أو لم تعالج كل تحدياتها التقنية والبيئية. ويحاول النظام الدولي أن يتجاهل أهمية تلك الرسالة ويحذر مخاطرها عليه. ويرى خبراء إن الانتقال إلى اقتصاد رقمي بالكامل دون معالجة التحديات التقنية وتحديث أنظمتنا التعليمية هو وصفة كارثية^(٢).

لكن العملات الرقمية المشفرة هي هدف وأداة جرمية للمجرمين في آن واحد، فهؤلاء يبتكرون يومياً وسائل وطرقاً حديثة لتنفيذ مخططاتهم التي تتناول العملات الرقمية الافتراضية. في حين أنّ غياب التشريعات التنظيمية والعقابية يسهم في إفلات هؤلاء من الملاحقة الجزائية والعقاب. وفي هكذا حال، يقف المتضرر من دون حماية قانونية وغياب أي وسيلة لإعادة أمواله المنهوبة أو حقوقه المهذورة. ويرى بعض الخبراء أنّ البيتكوين والعملات الافتراضية أطلقت عنان الأسواق السوداء الإلكترونية، فأصبحت الجرائم المنظمة والاقتصادية والمالية أكثر تعقيداً في السنوات الماضية^(٣).

(١) تعتبر أول استراتيجية داخلية لمنظومة الأمم المتحدة بشأن هذا الموضوع، في تحديد الكيفية التي سيدعم بها النظام استخدام التكنولوجيات الجديدة للتعبيل بإنجاز ولاياته لا سيما خطة عام ٢٠٣٠. يشرح القسم الأول من الاستراتيجية خمسة مبادئ لتوجيه مشاركة الأمم المتحدة في التكنولوجيات الجديدة بينما يتناول القسم الثاني بالتفصيل أربع التزامات. ترتبط المبادئ الخمسة بالالتزام بالقيم العالمية ودعم الشفافية وتعزيز الشراكات والحفاظ على عقلية التعلم. وقد وضعت تلك المبادئ لتوجيه عمل الأمم المتحدة أثناء تعاملها مع التكنولوجيات الجديدة مثل العملات المشفرة والتقنية الحيوية والذكاء الاصطناعي. الالتزامات الأربعة في الاستراتيجية هي:

(١) تعميق القدرات الداخلية للأمم المتحدة والتعرض للتقنيات الجديدة؛

(٢) زيادة التفاهم والمناصرة والحوار حول التكنولوجيات الجديدة؛

(٣) دعم الحوار حول الأطر المعيارية والتعاونية؛

(٤) تعزيز دعم منظومة الأمم المتحدة لتنمية القدرات الحكومية في هذه المجالات.

(٢) كاثي موليان، تقنية سلسلة الكتل "البلوك تشين" والنمو المستدام، تشرين أول ٢٠٢٢ موجود على الموقع

<https://www.un.org/ar/44863>

(٣) Lydia Smith, "Coincheck: World's largest cryptocurrency theft worth £380m reported in Japan", Independent, 28 January 2018. -<https://www.independent.co.uk>

ويرتكب الجرائم الإلكترونية أفراد أو منظمات، وبعض هؤلاء المجرمين الإلكترونيين منظمين ويستخدمون التقنيات المتقدمة والانترنت السوءاء وهم ذوي مهارات فنية عالية، وبعضهم مجرد مخترقين مبتدئين.

تشمل أنواع الجريمة الإلكترونية الحديثة الأمرين التاليين أو أحدهما على الأقل نشاط إجرامي يستهدف أجهزة الكمبيوتر باستخدام الفيروسات وأنواع أخرى من البرمجيات الخبيثة، ونشاط إجرامي يستخدم أجهزة الكمبيوتر لارتكاب جرائم أخرى⁽¹⁾. وأظهرت الأبحاث أن حوالي ثلث سكان العالم يمكنهم فهم البيانات والإحصائيات التي تشكل مخرجات حركة البيانات المفتوحة فقط. ولكن تقنية البلوكتشين تذهب إلى أبعد من ذلك بكثير حيث تتطلب من المواطنين قبول نهجا جديدا لإدارة البيانات وأن يكون لديهم بعض الفهم للتشفير ومبادئ الإدارة الرئيسية أو مواجهة خسارة أموالهم أو خدماتهم الحكومية وهذا يحتاج الى علم ومعرفة لا تتم الا وفق خطة على المدى المتوسط والبعيد. ومن هنا الدعوة دوما الى التكاتف الدولي والمباشرة بالحلول لخطورة تأثير الجرائم المرتكبة في دولة على مصالح أفراد وهيئات في دول أخرى.

وسنبحث في الفصل الاول مساهمة العملة الرقمية في الجرائم، وفي الفصل الثاني التجربة اللبنانية مع العملات المشفرة، وخاتمة مع المقترحات.

○ الفصل الاول: مساهمة العملة الرقمية في الجرائم

ترتكب أغلب جرائم الانترنت على أيدي القراصنة وهم لصوص أو مخترقين يودون تغيير واقعهم أو كسب الأموال، أو تبييض أموال غير مشروعة أو تمويل إرهاب عبر الدول دون المرور بالحدود الجغرافية، وأحيانا نادرة أخرى يكون الهدف من وراء جرائم الإنترنت هو إلحاق الضرر بالافراد أو الهيئات أو بأجهزة الكمبيوتر لأسباب غير الربح، وقد تكون هذه الأسباب سياسية أو شخصية. وقد وجد المجرمون العملة المشفرة وسيلة واداة فاعلة للتداول نظرا لطبيعتها وتحقيق الجرائم الإلكترونية، وتسيير النشاط الإجرامي كما أنها أصبحت هي نفسها محل استهداف المجرمين ومحل الجرائم.

سنبحث في فقرة أولى أنواع العملات الرقمية، وفي فقرة ثانية الجرائم الواقعة على العملة الرقمية.

⁽¹⁾ الاحتيال عبر البريد الإلكتروني والإنترنت.

تزوير الهوية (حيث تتم سرقة المعلومات الشخصية واستخدامها)

سرقة البيانات الشخصية المالية أو بيانات الدفع بالبطاقة أو بيانات الشركة وبيعها.

الابتزاز الإلكتروني (طلب المال لمنع هجوم مهدد) وهجمات برامج الفدية (نوع من الابتزاز الإلكتروني)

السرقة المشفرة (حيث يقوم المتسللون بتعدين العملات المشفرة باستخدام موارد لا يملكونها)

التجسس الإلكتروني (حيث يتمكن المتسللون من الوصول إلى بيانات الحكومة أو الشركة).

التدخل في الأنظمة بطريقة تعرّض الشبكة للخطر - انتهاك حقوق النشر - المقامرة غير المشروعة.

بيع السلع غير المشروعة عبر الإنترنت - طلب مواد إباحية تستغل الأطفال أو إنتاجها أو امتلاكها.

• فقرة أولى: أنواع العملات الرقمية

جذب سوق العملات الرقمية باختلاف أنواعها اهتمام مختلف الفاعلين في الأسواق الاقتصادية والاستثمارية من رجال أعمال وشركات، واهتمت الحكومات بالعملية الرقمية وشجعت التعاملات بالوسائل الإلكترونية كقيمة إضافية للنقود المعدنية والورقية. ولكن هذه العملات عرضة لتقلبات شديدة، وانخفض سعر أقدام وأكبر عملة رقمية، وهي البيتكوين بنسبة ١١% في ١٧ أيار ٢٠٢٢، وانخفض بأكثر من ٥٠% منذ تشرين الثاني ٢٠٢١. ويُعدّ الهبوط العام في الأسواق أحد أسباب انخفاض قيمتها. وذلك بسبب انهيار عملة لونا وعملة التيرا التي كانت إحدى أفضل خمس عملات مستقرة نظراً لارتباطها بالدولار. وترتبط العملات الرقمية ببعضها وتؤثر على نمط الأسواق فمثلاً عملة تيثرت ترتبط بالدولار أيضاً، حيث تستبدل كل وحدة منها بدولار، وأي تراجع لها يؤثر على جميع الأسواق التي تشهد تداولاً مقابل تيثرت حيث تشير بعض التقديرات إلى أن ما يصل إلى ٧٠% من مشتريات البيتكوين تُجرى باستخدام هذا البديل الرقمي للدولار^(١). ومن جهة أخرى، أظهرت أسواق العملات الرقمية قدرة غير عادية على البقاء، ونجت من عدة تجارب جعلتها على وشك الموت في الماضي، مثل الهبوط بنسبة ٣٠% في يوم واحد عام ٢٠٢١ كرد فعل على إجراءات تنظيمية صارمة اتخذتها الصين. وهذه التقلبات تدفع بالدول والمؤسسات الاستثمارية المتحفظة على التداول بالعملية المشفرة بعدم الاستثمار فيها بالمستقبل، حيث يبدو لها أن قضية اعتماد المؤسسات للعملات الرقمية تتراجع يوماً بعد يوم، فالمجال لا يوفر ملاذاً آمناً بل تنوعاً سلبياً فقط عبر مخاطر غير اعتيادية. وسنعرض أولاً للتعاملات المالية الإلكترونية، وثانياً للعملات الرقمية الحكومية، وثالثاً للعملات الافتراضية أو المشفرة.

■ أولاً: التعاملات المالية الإلكترونية

تتم التعاملات الرقمية عبر وسطاء مثل المصارف والمؤسسات المالية، والتي تتحمل أعباء تأمين المعاملات والتأكد من عدم وجود أي تلاعب أو تحايل لضمان سلامة المعاملات وينتج عن هذا التدخل بعض التأخير والمصاريف الإضافية على عاتق المستخدمين. وتستخدم التعاملات المالية الرقمية بشكل واسع البطاقات الائتمانية أو خدمات المدفوعات والتحويلات الإلكترونية، ويمكن لأي شخص الدفع بواسطة البطاقات الائتمانية بأنواعها في المحلات التجارية أو على مواقع التسوق الإلكتروني، وكذلك الدفع أو التحويل عبر خدمات شركات مالية متخصصة مثل PayPal. كما أن التعاملات المالية الرقمية تعتمد على تداول أموال حقيقية، ولكن بشكل إلكتروني، وبذلك فإن الطرفين، المرسل والمستقبل أو المشتري والتاجر،

^(١) لورنس فليشر وآدم سامسون، مقال، الأسبوع الذي هزّ عرش العملات الرقمية، فاينانشال تايمز، ١٧ أيار ٢٠٢٢ موجود على موقع <https://www.wamda.com/ar/2022/05/week-shook-crypto-arabic>

يعتمدون على القيمة الفعلية للأموال التي يتم التعامل بها، مضافاً إليها مصروفات الدفع أو التحويل والتي تتمثل في تكلفة التحويل، وكذلك تكاليف معالجة بيانات الحركات المالية وتأمينها. وقد تكون التعاملات خاصة بين المصارف وفق نظام سويفت المصرفي الخاص.

■ ثانياً: العملات الرقمية الحكومية

تفرض العملات الرقمية نفسها ويتم تداولها والتعامل بها على شبكة الإنترنت كبديلة للنقود التقليدية سواء ورقية أو معدنية. وعرف التوجيه الأوروبي النقود الإلكترونية أي النقود التقليدية المستعملة في المعاملات الإلكترونية. ويعم هذا الاتجاه جميع الدول حول العالم حالياً التي باتت تعتمد العملات الرقمية بدلاً من النقود التقليدية من أجل تخفيض تكاليف طباعة وصك النقود والمحافظة على قيمة العملة المحلية، وتسهيل المدفوعات والتحويلات المالية الإلكترونية. يشمل مصطلح العملات الرقمية وفق تقرير مجموعة العمل المالي FATF أولاً النقود الإلكترونية أي الـ E-Money، وثانياً العملات الافتراضية أي الـ Virtual Currency أي الموجودة فقط بطبيعة رقمية ومن ضمنها العملات المشفرة⁽¹⁾.

وتعتبر المركزية والسيطرة الحكومية ومعرفة هوية المستخدمين، من أهم العوامل لاعتماد العملات الرقمية، حيث إن الدول تكون معها قادرة على أن تكون المصدر المركزي الرئيسي والمنظم لاستخدامها، كما أن ذلك يجعلها قادرة على التصدي لأي استخدامات غير قانونية أو إجرامية مثل تبييض الأموال أو تمويل الإرهاب والتداول عبر الشبكة السوداء.

بدأت الصين تطبيقاً تجريبياً مع بداية العام ٢٠٢٢ لعملتها المشفرة اليوان الرقمي "e-CNY" كبديل عن الأموال التقليدية، وذلك باستخدامات الهواتف الذكية التي تعمل بنظامي أندرويد و IOS ، بحيث يسهل على المستخدمين التعامل بها من هواتفهم المحمولة. وكذلك فعل البنك المركزي الكندي بعدة مبادرات رقمية وأشهرها Project Jasper والذي يعتمد على نفس فكرة بقية العملات الحكومية الرقمية، بحيث تعتمد على إصدار البنك المركزي الحكومي للبدل الرقمي لعملة الدولة، على أن تكون الوحدة الواحدة من العملة المادية الحقيقية تساوي عملة واحدة من نظيرتها الرقمية. وبدأ الاتحاد الأوروبي في التخطيط لإطلاق "اليورو الرقمي" خلال الفترة المقبلة، حيث وضع الأسس الرقمية من أوراق بحثية ومناقشات مع مختلف الجهات، ولكن الأمر لم يدخل بعد في حيز التطبيق التجريبي⁽²⁾. وكانت تحضيرات جدية من مصرف لبنان لإصدار عملة لبنانية رقمية مع نهاية عام ٢٠١٩ وحالت الظروف دون ذلك.

■ ثالثاً: العملة الافتراضية أو المشفرة

(1) Financial Action Task Force (Report): "Virtual Currencies Key Definitions and Potential AML/CFT Risks", France, June 2014

موجود على الموقع التالي <http://www.fatf-gafi.org/publications>

(2) <https://alwatannews.net/Business/article/983545>

تعتبر العملات المشفرة جزءاً من العملات الرقمية ولكن ذات طبيعة خاصة، ولا تصدرها جهات رسمية ولا تخضع لقوانين معينة بالذات، وتعتمد على بروتوكولات تشفير معقدة داخل سلاسل الكتل Blockchain، وهو نظام شبيه بنظام التداول المصرفي الدولي السويفت (SWIFT) وهو أكثر تعقيداً. ويتم التشفير من خلال إجراء حسابات دقيقة وطويلة. ويتم تقسيم بيانات التداول إلى كتل لمعالجة العدد الهائل لعمليات التداول الحاصلة (حوالي ١٦.٥ مليون عملية يوميا)، حيث لا يستطيع كمبيوتر واحد القيام بكل هذا. ويتم توزيع الكتل عبر الشبكة على كمبيوترات وأجهزة التعدين المنتشرة حول العالم، والتي تقوم بمعالجة هذه البيانات من خلال عمليات رياضية، وتبقي هوية المتداولين سرية وبدون أسماء أو عناوين. وترتبط جميع عمليات العملات المشفرة بالرمز المتسلسل للمحافظة التي تم استخدامها، وهذا الرمز يتكوّن من مجموعة من الأرقام والحروف المتداخلة^(١).

ويقوم هذا النوع من العملات الرقمية على فكرة لامركزية القرار، فليس هناك طرف واحد يتحكم في حركة وإصدار العملات المشفرة، لأن تلك العملات يمكن الحصول عليها من خلال التعدين، والذي يعتبر نقطة القوة بالنسبة لتلك العملات. ويؤكد خبراء استحالة تقنية لتقليد هذه العملات وتزويرها^(٢). فعملية تعدين العملات تتمثل في حل مجموعة من العمليات الحسابية وتشفير معقد جداً، وعندما يصل أحد العاملين في التعدين بأجهزته الحاسوبية لمعالجة تلك الكتلة، يحصل على مكافأة من العملة ذاتها. ويحتاج الجهاز لانتهاه من معالجة كتلة واحدة من البيانات حوالي عشرة دقائق، ويتلقى بعدها المعدن المكافأة بالعملات الافتراضية. إلا أن إنتاج عملة واحدة من البيتكوين على سبيل المثال يحتاج إلى أكثر من سنة من العمل المستمر على مدار الساعة بحسب عدد كتل البيانات، وبذلك تستمر عمليات التعدين بقوة وثبات واستقرار. اعتمدت عدة دول العملات المشفرة وأصبحت البيتكوين عملة قانونية في السلفادور في شهر أيلول ٢٠٢١. وتشير تقديرات الفاينانشيل تايمز إلى أن السلفادور أنفقت أكثر من ١٠٠ مليون دولار على البيتكوين. وتتداول منصات وبورصات العملات والاسهم والمعادن والبتروال الاف العملات مشفرة.

ومنذ العام ٢٠١٧ تم اعتماد طريقة ICO لاطلاق العملات، وهي وسيلة غير منظّمة تُجمَع من خلالها الأموال من الجمهور لمشروع رمز أو عملة مشفرة جديدة تتأسس على البلوكشين، وتحولت Initial Coin Offering إلى طريقة رائدة عالمياً للتمويل الجماعي Crowdfunding للشركات الناشئة^(٣). فاكتمت

(1) Lyndsey Gilpin, "10 things you should know about Bitcoin and digital currencies", TechRepublic, 21 May 2014

(2) Chris Rose, "The Evolution Of Digital Currencies: Bitcoin, A Cryptocurrency Causing A Monetary Revolution", International Business & Economics Research Journal, vol.14, no.4, 2015, p.618

(3) Arjun Kharpal, "Tokenization: The World of ICO's", CNBC, 16 July 2018. – <https://www.cnbc.com>

عالم الأعمال والتجارة الدولية، وشكّلت نوعًا جديدًا من الشركات، إذ يتهافت أصحاب رؤوس الأموال على تأسيس شركات تطرح رموزًا Tokens و عملات مشفرة عن طريق ال ICO.

وتقوم حملة بيع العملات والرموز قبل اطلاق العملة الفعلي، إذ يُصار إلى عرضها للبيع أو الاستثمار من قبل الشركات الناشئة التي تلجأ إلى هذه الطريقة لتقادي العراقيل والصعوبات في الحصول على التمويل المناسب لمشاريعها من خلال المصارف وسائر المؤسسات المالية. خلال هذه الحملة تطرح العملة أو الرمز المعين، كما هو الحال عند طرح أسهم شركة معينة للاكتتاب، ليتمّ الشراء من قبل القائمين. تشير إلى أنه يمكن شراء هذه العملات بال نقد كالدولار أو بعملات مشفرة أخرى كالبيتكوين أو الإثيريوم.

من هذا المنطلق، يستحوذ المستثمر مباشرة على ال Token الخاصة بتلك ال ICO وينقلها إلى محفظته الإلكترونية الخاصة. وعند إطلاق المشروع رسميًا من قبل الشركة التي طرحت رموز ال ICO الخاصة بها، يحصل المستثمر على نسبة أرباح كما هي حال الأسهم، ويمكنه لاحقًا التداول بها واستعمالها كعملة لشراء السلع والخدمات^(١).

ويقوم المستخدمون بحجب هويتهم وعناوينهم نظرا لسهولة تتبع هوية كافة التعاملات والتحويلات التي يقوم بها أي شخص حقيقي يتعاطى العملات المشفرة بمجرد ربط أي عنوان لمحفظة الإلكترونية، لأنه لا يمكن حذف أي معاملات تتم داخل سوق العملات المشفرة بمختلف أنواعها، وجميعها يتم حفظها في سجلات عامة موزعة Distributed Ledger متاح للجميع الاطلاع عليها. ويمكن شراء العملات مباشرة من المنصات والمواقع والتطبيقات التي أصبحت متاحة بشكل واسع على مستوى العالم، وعند البيع والشراء يتحكم عنصر العرض والطلب في أسعار تلك العملات. وتكون تلك المواقع والمنصات هي المرجع في حال حصل أي مراجعات قضائية، ولذلك فهي تجبر المستخدمين على التوقيع على ابراء ذمة سابق للتعامل وتحفظ حقها باللجوء الى المحاكم وتوكيل محامين على نفقة المستخدم^(٢).

• فقرة ثانية: الجرائم الإلكترونية واستخدام العملة الرقمية

العملات الرقمية هي هدف للمجرمين وأداة جرمية في آن واحد، فهؤلاء يبتكرون يوميا وسائل وطرقًا حديثة لتنفيذ مخططاتهم التي تتناول العملات الرقمية الافتراضية. في حين أنّ غياب التشريعات التنظيمية والعقابية يساهم في إفلات هؤلاء من الملاحقة الجزائية والعقاب. وفي هكذا حال، يقف المتضرر من دون حماية قانونية وغياب أي وسيلة لإعادة أمواله المنهوبة أو حقوقه المهذورة. ويرى بعض الخبراء أن البيتكوين

^(١) ماريلين أوردikian، العملات الافتراضية المشفرة في الحقل الجنائي السيبراني، لعدد ١٠٨ - نيسان ٢٠١٩
<https://www.lebarmy.gov.lb/ar/content>

^(٢) شروط يوقع عليها من يريد دخول منصة بينانس ويعفيها من المسؤولية وتحدد قواعد المراجعة بطلبات المحاكم امام مكاتبها فقط
<https://www.binance.com/ar/binance-legal>

والعملات الافتراضية أطلقت عنان الأسواق السوداء الإلكترونية أو ما يعرف بالشبكة السوداء، فأصبحت الجرائم المنظمة والاقتصادية والمالية أكثر تعقيداً، في السنوات الماضية⁽¹⁾.
وسنعرض أولاً الجرائم الإلكترونية الحديثة وثانياً الجرائم الواقعة على العملة الرقمية.

■ أولاً: الجرائم الإلكترونية الحديثة

الجرائم الإلكترونية هي نشاط إجرامي يستهدف جهاز كمبيوتر أو شبكة كمبيوتر أو جهازاً متصلاً بالشبكة وتحاول استخدامهم. تقع معظم الجرائم الإلكترونية على أيدي القراصنة وهم لصوص أو مخترقين يودون كسب الأموال، وأحياناً نادرة أخرى يكون الهدف من وراء الجرائم الإلكترونية هو إلحاق الضرر بأجهزة الكمبيوتر لأسباب غير الربح، وقد تكون هذه الأسباب سياسية أو شخصية. ويرتكب الجرائم الإلكترونية أفراد أو منظمات، وبعض هؤلاء المجرمين منظمين ويستخدمون التقنيات المتقدمة وهم ذوي مهارات فنية عالية، وبعضهم مجرد مخترقين مبتدئين. تشمل أنواع الجرائم الإلكترونية الحديثة الأمرين التاليين أو أحدهما على الأقل نشاط إجرامي يستهدف أجهزة الكمبيوتر باستخدام الفيروسات وأنواع أخرى من البرمجيات الخبيثة، ونشاط إجرامي يستخدم أجهزة الكمبيوتر لارتكاب جرائم أخرى⁽²⁾.

إن مرتكبي الجرائم الإلكترونية الذين يستهدفون أجهزة الكمبيوتر قد يصيبنها ببرمجية خبيثة لإتلاف الأجهزة أو إيقافها عن العمل، وقد يستخدمون تلك البرمجية الخبيثة في حذف البيانات أو سرقتها. يمكن كذلك أن يعمل مرتكبو الجرائم الإلكترونية على منع المستخدمين من استخدام موقع إلكتروني أو شبكة أو منع شركة تقدم خدمة برمجية أو عبر الانترنت من الوصول إلى عملائها، وهذا الأسلوب معروف باسم هجوم الحرمان من الخدمات (DoS).

قد تشمل الجريمة الإلكترونية التي تستخدم أجهزة الكمبيوتر لارتكاب جرائم أخرى استخدام أجهزة الكمبيوتر أو الشبكات لنشر البرامج الضارة أو المعلومات أو الصور غير المشروعة.

غالباً ما يفعل مرتكبو الجرائم الإلكترونية الأمرين في الوقت نفسه. قد يستهدفون أجهزة الكمبيوتر التي تحتوي على فيروسات أولاً ثم يستخدمونها لنشر البرمجيات الخبيثة على أجهزة أخرى أو عبر الشبكة. توجد

⁽¹⁾ Lydia Smith, "Coincheck: World's largest cryptocurrency theft worth £380m reported in Japan", Independent, 28 January 2018. -<https://www.independent.co.uk>

⁽²⁾ الاحتيال عبر البريد الإلكتروني والإنترنت.

تزوير الهوية (حيث تتم سرقة المعلومات الشخصية واستخدامها)

سرقة البيانات الشخصية المالية أو بيانات الدفع بالبطاقة أو بيانات الشركة وبيعها.

الابتزاز الإلكتروني (طلب المال لمنع هجوم مهدد) وهجمات برامج الفدية (نوع من الابتزاز الإلكتروني)

السرقة المشفرة (حيث يقوم المتسللون بتعدين العملات المشفرة باستخدام موارد لا يملكونها)

التجسس الإلكتروني (حيث يتمكن المتسللون من الوصول إلى بيانات الحكومة أو الشركة).

التدخل في الأنظمة بطريقة تعرّض الشبكة للخطر - انتهاك حقوق النشر - المقامرة غير المشروعة.

بيع السلع غير المشروعة عبر الإنترنت - طلب مواد إباحية تستغل الأطفال أو إنتاجها أو امتلاكها.

كذلك بعض البلاد التي تضع فئة ثالثة من الجرائم الإلكترونية حيث يتم استخدام أجهزة كمبيوتر كملحق في الجريمة. من أمثلة ذلك استخدام أجهزة كمبيوتر لتخزين البيانات المسروقة.

وتزداد بشكل رهيب سرقة البيانات وسرقة الهوية، وبحسب تقرير حالة مرونة الأمن السيبراني لعام ٢٠٢١ زادت الهجمات الأمنية بنسبة ٣١٪ من ٢٠٢٠ إلى ٢٠٢١، وزاد عدد الهجمات لكل شركة من ٢٠٦ إلى ٢٧٠ على أساس سنوي. إن الهجمات على الشركات تؤثر على الأفراد أيضاً لأن العديد منهم يخزنون بيانات حساسة ومعلومات شخصية من العملاء. وهناك تطبيقات مفخخة تتواجد طبيعياً على غوغل، وعند تنزيلها كبروات تعريفية تسرق كل البيانات الشخصية على الشبكة الاجتماعية^(١). كما يتم ذلك على نطاق اوسع وبشكل دوري لشركات التواصل الاجتماعي، واهمها فايسبوك حيث تأثر عام ٢٠١٩ أكثر من ٢٦٧ مليون مستخدم، وكان آخرها حظر مليون شخص بتاريخ ٢٠٢٢/١٠/٨^(٢).

يمكن لهجوم واحد سواء كان خرقاً للبيانات أو برمجيات خبيثة أو برنامج طلب فدية أو هجوم حرمان من الخدمات أن يكلف الشركات من جميع الأحجام ما متوسطه ٢٠٠ ألف دولار، وتخرج العديد من الشركات المتضررة من العمل في غضون ستة أشهر من الهجوم، وذلك وفقاً لشركة Hiscox للتأمين^(٣). ونشرت Javelin Strategy & Research دراسة عن احتيال الهوية في عام ٢٠٢١ وجدت فيها أن خسائر الاحتيال في الهوية لذلك العام بلغت ٥٦ مليار دولار. يمكن أن يكون تأثير الجريمة الإلكترونية بالنسبة للأفراد والشركات عميقاً وضرراً مالياً في المقام الأول، ولكن أيضاً فقدان الثقة والإضرار بالسمعة.

وهناك قدرة هائلة لمجرمي الشبكات على استخدام العملات الرقمية للتداول والتبادل عبر الإنترنت في الشبكة السوداء، وتوفير غطاء مالي دون هوية أو عنوان لبيع الممنوعات كالمخدرات والأسلحة، وتقديم الخدمات غير المشروعة كالاتجار بالأشخاص والأسلحة والأعضاء البشرية، وتبييض الأموال وتمويل الإرهاب^(٤). وأصدرت وكالة اليوروبول في ١٧ أيار ٢٠٢٢ تنكيراً بعمليات النصب والاحتيال التي انتشرت في السوق، عندما وضعت الوكالة روجا إيغناطوفا، مخترعة عملة وان كوين (onecoin) على قائمة الهاربين المطلوبين، وذكرت الوكالة أن هذه الهاربة حثت مستثمرين من جميع أنحاء العالم على الاستثمار في عملة لا قيمة لها في الواقع. وقالت وكالة اليوروبول إن مخطط هذه الهاربة تسبب في خسائر تصل على الأرجح إلى عدة مليارات من الدولارات.

ولا بد من الإشارة ان هناك عالم يتمدد ببطءٍ وصمت، ويحمل في طياته تهديدات جديدة، تختلف خطورتها تبعاً للتطور التكنولوجي لكل دولة، وهو يُعرف بالشبكة السوداء (Dark Web). فالتكنولوجيا

^(١) <https://me.kaspersky.com/resource-center/threats/what-is-cybercrime>

^(٢) تطبيقات مفخخة تسرق كلمات المرور على فايسبوك <http://amp.dw.com>

^(٣) <https://www.hiscox.co.uk/>

^(٤) انظر تقرير اليوروبول ٢٠٢١ ومجموع الجرائم التي ترتكب ومساهمة العملات المشفرة فيها موجود على الموقع https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2021.pdf

ووسائل الاتصالات الآخذة بالتوسع بسرعة كبيرة لديها القابلية لتوفير أدوات قوية وفعّالة بهدف إنشاء أسواق رديفة على الشبكة السوداء لتجارة افتراضية تعتمد بالدرجة الأولى على الثقة المتبادلة بين أطرافٍ ثلاثة: البائع والمشتري والوسيط، تدّعي ضمان سرية الهوية الشخصية، مما يُبقي الأطراف بعيدين نسبيًا عن نطاق عمل أجهزة إنفاذ القانون. وتنتشر على الشبكة السوداء عدة أسواق متخصصة ببيع مختلف أنواع المخدرات والسلاح، إضافة للمواد الإباحية ولأئحة طويلة بالمواد الممنوعة التي قد تغري كثيرين للدخول إليها، بدافع الفُصول في البداية، والسعي بعدها الى جمع المال السهل والانخراط في التداولات غير الشرعية دون الالتفات الى مخاطر التورط في الجرائم.

يزداد نمو هذه الاسواق السوداء وفق آخر التقديرات بشكلٍ مستمر لعدة أسباب، منها تزايد التجارة بالعملات المشفرة (بيتكوين وغيرها)، وانتشار منتديات القرصنة والخدمات التي تقدمها، إضافة للكثير من الخدمات كبيع الآثار المسروقة والمهربة، والتجارة والمضاربة بالعملات الرقمية، ومضاربات البورصة غير الشرعية وتبييض الأموال الذي يعتبر سوقاً مغرية للباحثين عن الربح السريع⁽¹⁾.

■ ثانياً: استخدام العملة الرقمية في جرائم الانترنت

تستخدم العملات الرقمية في جرائم الانترنت وكذلك خارج الفضاء السيبراني. ويستخدم المجرمون العملة المشفرة في غسيل الأموال وتمويل الإرهاب، والاتجار بالبشر، وجمع البيانات الرقمية بطريقة غير شرعية أو من دون تصريح، وإساءة استخدامها من قبل الحائز، والولوج إلى نظام معلوماتي والإقدام على نسخها، تعديلها أو إلغائها، والتعدّي على سرّيتها عن طريق نشرها أو تسريبها أو إفشائها لأشخاصٍ غير مخوّلين الاطلاع عليها. أما العلاقة الجوهرية بين هذه البيانات الرقمية والعملات الافتراضية فتتكرّس بالتقائها في العالم الجرمي على الشبكة السوداء. وتُفتَرَف الأفعال الجرمية ذات الصلة بالعملات الافتراضية عن طريق استغلال البيانات الشخصية الرقمية المسروقة أو المجمعّة من دون تصريح، كأداةٍ جرمية تسهّل اقتراف جرائم على حائزي هذه العملات.

أبلغت وكالة الأمن السيبراني وأمن البنية التحتية الأمريكية (CISA) عن زيادة هائلة بنسبة ٦٢٪ سنويًا في قضايا الجرائم الإلكترونية بين شباط ٢٠٢١ وشباط ٢٠٢٢. وبشكل عام، توجد ٣ مستجدات عندما يتعلق الأمر بالجرائم الإلكترونية في عام ٢٠٢٢ مقارنة بالسنوات السابقة، هي أولاً التركيز الكبير على العملات المشفرة، وثانياً المزيد من الهجمات الموزعة على الشركات الصغيرة، وثالثاً زيادة التنوع في عمليات الاحتيال لسرقة الهوية.

(1) محمد الصغير، ياسر الموسوي، مقال DARK WEB: الوجه المظلم للإنترنت السبت ٢٠ آب ٢٠٢٢ موجود على الموقع <https://al-akhbar.com/Lebanon/343405>

وكشف تقرير نشره موقع hespress، عن وصول القيمة الإجمالية لجرائم العملات الرقمية في العالم خلال العام ٢٠٢١ إلى مستوى قياسي قدره ١٤ مليار دولار تقريباً^(١). وأشار التقرير إلى أن إحدى شركات الاستشارات العالمية، قد كشفت عن أن هذه القيمة الإجمالية تقدر بأقل من ١% من إجمالي حجم تعاملات العملات الرقمية المشفرة خلال العام نفسه^(٢).

ونوه التقرير الذي حمل عنوان "تقرير جرائم العملات الرقمية ٢٠٢٢"، إلى ارتفاع إجمالي حجم التعاملات بالعملات الرقمية في العالم في العام ٢٠٢١ إلى ١٥.٨ تريليون دولار، أي بمقدار ٥٠٠% مقارنة بالعام السابق، منها إلى أن ٠.١٥% من هذه التعاملات تمت لأغراض غير مشروعة. وقال رئيس إدارة الأبحاث في الشركة kim grawer إن قيمة جرائم العملات الرقمية وصلت إلى مستوى قياسي من الناحية المطلقة، لكن نسبتها إلى إجمالي حجم تعاملات هذه العملات في العام الماضي تراجعت إلى أقل مستوى. وسنعرض بعضاً من أكثر الأفعال الجرمية شيوعاً والتي تتناول العملات الافتراضية:

١- السرقة المشفرة

تبرز عملات مشفرة جديدة بالتعدين وهو كما ذكرنا عبارة عن مشاغل وصناعة يقوم بها المهتمون بغية معالجة وحفظ سلاسل الكتل وإصدار عملات جديدة. ويقوم القراصنة بتعدين العملات المشفرة باستخدام موارد وكمبيوترات لا يملكونها وهو ما يعرف بالسرقة المشفرة (Cryptojacking)، وهي استخدام كمبيوتر الغير دون علمه لتعدين العملات المشفرة عبر برامج معينة. تشكل السرقة المشفرة أو التعدين غير المشروع تهديداً جدياً على المؤسسات والأشخاص. وفي ظل ارتفاع عدد العملات المشفرة وكثرة اعتمادها في الأسواق. وتهتم الوكالة الوطنية للأمن السيبراني في بريطانيا (NCSC) بهذا النوع من السرقات وأصدرت تقارير سنوية منذ ٢٠١٨ تحذر فيها من ارتفاع عدد ضحايا هذه السرقات وصعوبة كشف المتسللين وتزايد أعدادهم كما ورد في تقرير ٢٠٢١^(٣).

٢- جريمة السرقة

إن جريمة سرقة العملات الافتراضية والمشفرة هي الأكثر انتشاراً، بحيث إن معظم منصات التداول والمحفظات الإلكترونية أو الصلبة التي تخزن العملات، هي عرضة للسرقة. وفي ظل الارتفاع الهائل لعدد هذه المحفظات، فقد تجاوزت المبالغ المسروقة ملايين الدولارات، والوثيرة إلى ارتفاع. ففي شهر كانون الثاني من العام ٢٠١٨ مثلاً، تمت سرقة ما يقارب الـ ٥٢٣ مليون دولار أميركي من منصة التبادل اليابانية الشهيرة

(1) <https://en.hespress.com>

(2) Chainalysis: The Blockchain Data Platform <https://www.chainalysis.com> موجود على الموقع

(3) https://webarchive.nationalarchives.gov.uk/ukgwa*/https://www.ncsc.gov.uk/report/weekly-threat-report-1st-october-2021

Coincheck بعد تعرّضها للقرصنة من قبل مجهولين^(١). وفي قضية سرقة العملات الرقمية كانت الاولى من نوعها في الامارات العربية تمت سرقة ٢٥ بيتكوين عبر تحويلها من حساب الى حساب بالقوة وقد وصلت هذه القضية الى خواتيمها وتم تجريم الفاعلين^(٢).

السرقة تتضمن التصيد الاحتيالي باستخدام رسائل بريد إلكتروني أو صفحات ويب جديدة بالثقة لخداع الأشخاص من أجل النقر فوق الارتباط أو تقديم معلوماتهم الشخصية، وتسمح هجمات التصيد الاحتيالي الناجحة لمجرمي الإنترنت بسرقة الأموال أو الهوية. ويكون معدل نجاح هجمات التصيد الاحتيالي منخفضاً مع برامج الأمان والحماية، ولكن مع وجود أكثر من ١٠٠ مليون هجوم يوميًا، فلا عجب أن يتمكن بعض المهاجمين من الوصول إلى أهدافهم. وقد سُرق ٥٠ مليون دولار أميركي من موقع Blockchain.info ويُعدّ من أبرز المواقع التي توفّر خدمة المحفظات الإلكترونية عن طريق إدراج إعلانات خادعة على محرك غوغل^(٣).

٣- جريمة الاحتيال

جريمة الاحتيال هي من الجرائم الأكثر انتشارًا في العالم الافتراضي، بحيث يبتكر المجرم المعلوماتي وسائل جديدة ومتنوعة وفاعلة للإيقاع بالأشخاص. إن معدل الاحتيال في عالم العملات الافتراضية يندرج بالخطر، وذلك من جراء ارتكابها بشتى الطرق، سواء عن طريق حسابات تويتر وهمية تدّعي تحويل عملات مجانًا أو بإرسال رسائل بريد إلكترونية وهمية لمستثمري هذه العملات. وقد رفعت لجنة The Commodity Futures Trading Commission الأميركية، شكاوى ضد شركتين بتهمة الاحتيال في مجال بيع الاستشارة وتقديمها للاستثمارات في العملات الافتراضية. وفي الوقائع، كانت الشركتان تقدمان على إطلاق الوعود الكاذبة والأرباح والعوائد الوهمية^(٤).

وفي العالم العربي، استعادت الشرطة الإماراتية في إمارة الشارقة أكثر من مليوني درهم، في جريمة احتيال ارتكبت عن طريق بيع البيتكوين ٢٠١٩. ولقد تمّ الاستيلاء على المبلغ عن طريق الاحتيال من قبل شخصين، نجحوا بإيهام الضحية ببيعه عملة البيتكوين التي تعادل قيمتها مليونين وخمسمئة درهم. وتساهم

(1) National Cyber Security Centre, and National Crime Agency (Report): “The Cyber Threat to UK Business”, London, 2017-2018.- <https://www.ncsc.gov.uk>

(2) <https://www.albayan.ae/across-the-uae/accidents/2018-11-26-1.3419218>

(3) Sylvan Lane, “CFTC files charges in two cryptocurrency fraud cases”, The Hill, 19 January 2018. <https://thehill.com>

(4) The European Securities and Markets Authority-ESMA (Statements): “ESMA HIGHLIGHTS ICO RISKS FOR INVESTORS AND FIRMS”, 13 November 2018. The European Securities and Markets Authority-ESMA (Statements): “ESMA HIGHLIGHTS ICO RISKS FOR INVESTORS AND FIRMS”, 13 November 2018.- <https://www.esma.europa.eu>

الخبرة التكنولوجية والتخصص في ضبط المجرمين حيث تم القبض على متصيدين الكترونيين ضمن ساعات معدودة ٢٠٢٢^(١).

وفي لبنان حدثت جريمة احتيال أو بونزي الكتروني عام ٢٠٢١، حيث نشط سوق التداول بالعملات الرقمية في لبنان بعد انهيار القطاع المصرفي، ومعه ارتفعت نسبة حالات الاحتيال المرتبطة بهذه العملات. وتعرف هذه العمليات باسم «بونزي»، وهو أسلوب احتيال مالي يُمارس في كثير من الدول خصوصاً التي تعاني من أزمات اقتصادية ومصرفية.

تلقي هذه الطريقة نجاحاً كبيراً لدى الباحثين عن المال السهل والكسب السريع، والغريب انها تتطلب على مختلف الشرائح، وهي تتلخص بإيداع مبلغ من المال لدى شركة يُفترض أنها تقوم باستثماره واعطاء المُستثمر جزءاً من الأرباح. أول من استعمل هذه الطريقة كان تشارلز بونزي، في الولايات المتحدة عام ١٩٢٠، وتمكّن من كسب مبالغ كبيرة من خلال المتاجرة بقسائم تستعمل لبيع الطوابع البريدية.

تشكّل العملات الرقمية والمضاربات غير الشرعية وتبييض الأموال سوقاً مغرية للباحثين عن الربح السريع منذ سنوات. لم يكن لبنان بعيداً عن هذا النوع من العمليات، فنهاية عام ٢٠٢١ أنشئت منصة تحت اسم بينانس فند binancesfund تتعامل بعملة اليوأس دتي USDT، ويودع فيها المُستثمر دولاراته بعد ان يحولها إلى USDT، على ان يجني جزءاً من الأرباح. وبالفعل، حقّق بعض المستثمرين ارباحاً في البدايات، قبل أن تُقفل المنصة وتختفي الأموال. مما يذكر أن بعض الضحايا أكدوا أنهم كانوا يدركون منذ البداية بأن المنصة عبارة عن عملية بونزي، إلا أنهم رغم ذلك استثمروا فيها.

٤- العرض الاولي للعملة المشفرة

يبدع قراصنة الشبكة في مجال المال والعملات المشفرة إذ انخرطوا بعمليات بونزي وإختلاس واحتيال مستحدثة وفق رهان على التوجه العام لدى فئة الشباب خاصة للربح السريع. ونجح النصابون بتحصيل ملايين الدولارات عن طريق الاستثمار بعملة قيد التأسيس وما بات يعرف العرض الاولي للعملة المشفرة (Initial Coin Offering) ICO، حيث يقوم المستثمر الوهمي بإنشاء منصات لشركات بيع الرموز والعملات الوهمية والتي لا تستوفي شروط الحماية والموثوقية وتكون معرضة للسقوط. تبين أن معظم هذه المنصات والشركات وهمية وتهدف فقط إلى جمع المال عن طريق الاحتيال والنصب، وقد تخطت تداعياتها الحدود الجغرافية كافة نظراً لكونها عابرة للحدود.

ولقد حذرت السلطات الأميركية من خطر التعامل مع الـ ICO، فهذه الأخيرة تقع خارج النطاق القانوني الشرعي على غرار عدم توفيرها أي حماية قانونية للمستثمرين. واعتبرت السلطات أنّ الـ ICO غالباً ما تُستعمل في عمليات الاحتيال والخداع وتبييض الأموال^(١).

^(١) ضبطت القيادة العامة لشرطة الشارقة، في أقل من ثماني ساعات بعد تقديم البلاغ، متصيدياً إلكترونياً متخصصاً في النصب والاحتيال، استولى على ١.١ مليون درهم - <https://www.alkhaleej.ae/2022-08-21>

ولعل العام ٢٠١٨ شهد أكبر عمليات نصب وخداع في هذا المجال، فنذكر مثلاً شركة Bitconnect القائمة على الـ ICO، والتي نجحت في استقطاب الملايين من الدولارات، وبلغت قيمتها السوقية ٢.٧ مليار دولار أميركي، وتبين أنها شركة مخادعة، الأمر الذي أدى إلى هبوط سعر عملتها المشفرة لحين إعلان إفلاسها في شهر كانون الثاني من العام ٢٠١٨^(٢).

٥- تبييض الأموال وتمويل الإرهاب

ترتبط أجهزة مكافحة بين العملات المشفرة والجريمة المنظمة على الإنترنت الأسود، وهو ما تسعى العملات المشفرة لتجاوزه والدخول في النظام المالي التقليدي. فقبل ٢٠١١ لم تكن بيتكوين سوى عملة رقمية تستخدم غالباً على الإنترنت الأسود لتيسير المعاملات والتداول بين عصابات الجريمة المنظمة، وقراصنة الإنترنت للدفع والتحويل في عمليات طلب الفدية الرقمية أو تجارة المخدرات والدعارة والسلاح وغيره. تصدر النقود الورقية من قبل المصارف المركزية أو من جهات رسمية أخرى، على عكس العملات المشفرة التي تصدر بالتعدين. هذه الواقعة بحد ذاتها كانت مغرية للمجرمين. وحتى الآن، لا يزال القدر الأكبر من استخدام العملات المشفرة في الدفع هو في تلك المعاملات غير الشرعية. أما التداولات فيها بشكل شرعي، فهي في الأساس كاستثمار في أصل رقمي. وربما كان مكتب التحقيقات الفيدرالي الأميركي أكثر جهاز أمني في العالم لديه خبرة بتلك العملات المشفرة واستخداماتها غير الشرعية. فقبل ظهور تلك المشفرات خصوصاً بيتكوين للعلن وتعامل الجمهور فيها قبل نحو عقد من الزمن، كان المكتب يصادها ضمن حملاته على تجارة المخدرات، وتهريب البشر وكل أشكال الجريمة المنظمة الأخرى. وذكرت بعض التقارير في السابق أن مكتب التحقيقات الفيدرالي، ربما يملك أكبر كمية من عملة بيتكوين تقدر بالمليارات نتيجة تلك المصادر.

جعلت مجموعة العمل المالي (FATF) من أولوياتها التأكد من أن لا تصبح الأصول الافتراضية ملاذاً آمناً للتدفقات المالية التي تغذي الجريمة والإرهاب. وفي ايلول ٢٠٢٠ تم إصدار تقريراً عن الأصول الافتراضية ووضعت مجموعة العمل المالي مؤشرات لمعرفة غسل الأموال وتمويل الإرهاب وسيساعد القطاع الخاص على اكتشاف والإبلاغ عن المعاملات المشبوهة باستخدام الأصول الافتراضية. يسלט التقرير الضوء على المؤشرات الهامة التي يمكن أن تشير إلى سلوك إجرامي مثل الميزات التكنولوجية التي تزيد المجهولية باستخدام تبادلات الند للند في مواقع الويب، ومجهولية العملات الرقمية واستغلال المجرمين للبلدان الضعيفة التي تغيب فيها التدابير الوطنية.

(1) U.S. Securities and Exchange Commission <https://www.sec.gov>

(2) Tom Keating, David Carlisle and Florence Keen, "Virtual currencies and terrorist financing: assessing the risks and evaluating responses", TERR Committee of the European Parliament, 2018

وأوضحت مجموعة العمل المالي FATF في تقريرها ٢٠٢١ أنّ إرتباط العملات المشفرة بتبييض الأموال وتمويل الإرهاب لا يزال واضحاً^(١). فلقد تمّ الكشف عن عمليات تمويل لتنظيم الدولة الإسلامية ومجموعات إرهابية أخرى، فمثلاً برز حساب تابع لمنظمة إرهابية على موقع تويتر باسم Al Sadaqah لدعم الثوار في سوريا، ويقبل التبرعات بالعملات المشفرة، ولاحقاً ارتبط هذا الحساب بتنظيم القاعدة^(٢). والأخطر استغلال هذه العملات لارتكاب الجرائم المنظمة أيضاً، فعلى سبيل المثال أعلن مكتب الشرطة الأوروبية Europol أنّ الشرطة داهمت شبكة إجرامية مقرها في إسبانيا استخدمت بطاقات الائتمان والعملات المشفرة لتبييض ٨ مليون يورو حصيلة الإتجار بالمخدرات. وكانت الأموال التي يُصار إلى تبييضها تأتي من عصابات تهريب المخدرات في كولومبيا، ثم تُقسّم إلى مبالغ صغيرة وتودع في مئات الحسابات المصرفية^(٣).

أما في لبنان، فقانون مكافحة تبييض الأموال وتمويل الإرهاب رقم ٢٠١٥/٤٤ لا ينظرّق إلى هذه العملات، الأمر الذي يسهّل عمليات تبييض الأموال وتمويل الإرهاب، خصوصاً في ظل نظام السرية المصرفية. فكل ما لدينا هو تحذير صادر عن حاكم مصرف لبنان، يُنذر باستعمال هذه العملات لنشاطات إجرامية خاصة لتبييض الأموال وتمويل الإرهاب^(٤).

٦- الفدية الإلكترونية Ransomware

الفدية الإلكترونية هي نوع من البرمجيات الخبيثة التي تمنع المستخدمين من الوصول إلى نظامهم أو ملفاتهم الشخصية، وتطلب تسديد فدية من أجل استعادة الوصول. تُصطبح بالابتزاز والتهديد بتسريب أو محو معلومات وبيانات الضحية في حال تمّعت عن دفع الفدية المطلوبة^(٥).

احتجز هجوم برنامج الفدية Wannacry عام ٢٠١٧ آلاف أنظمة الكمبيوتر كرهائن إلى أن دفع الضحايا للمتسللين فدية بعملة البيتكوين. تجاوزت تكلفة الهجوم مدفوعات الفدية، فقد أسفر عن أضرار تقدر بنحو ٨ مليارات دولار في المستشفيات والبنوك والشركات في جميع أنحاء العالم. حدثت عدة هجمات الفدية الإلكترونية منذ ذلك الحين ويبدو أنها في ازدياد^(٦).

(١) التقرير السنوي لمجموعة العمل المالي ٢٠٢٠-٢٠٢١

<https://www.fatf-gafi.org/media/fatf/documents/brochuresannualreports/Annual-Report-2020-2021.pdf>

(٢) ماريلين أوردكيان، العملات الافتراضية المشفرة في الحقل الجنائي السيبراني، لعدد ١٠٨ - نيسان ٢٠١٩

<https://www.lebarmy.gov.lb/ar/content>

(٣) المرجع السابق

(٤) ماريلين أوردكيان، العملات الافتراضية المشفرة في الحقل الجنائي السيبراني، لعدد ١٠٨ - نيسان ٢٠١٩

<https://www.lebarmy.gov.lb/ar/content>

(٥) المرجع السابق

(٦) مجموعة العمل المالي، كيف يمكن للمجرمين إساءة استخدام الأصول الافتراضية

<https://www.fatf-gafi.org/publications/virtualassets/documents/virtual-assets>

ودفعت الشركة المالكة لخط أنابيب الوقود كولونيل بايبلين فدية لعصابة قرصنة إلكترونية. وأعلن مكتب التحقيقات الفيدرالي أنه تمكن من استرداد ٢.٣ مليون دولار من الفدية التي بلغت نحو ٥ ملايين دولار. وكانت الشركة تعرضت لهجوم قرصنة بفيروس إلكتروني في أيار ٢٠٢١ مصدره مجموعة قرصنة من أجل الفدية تدعى "داركسايد" (darkside). ودفعت الشركة الفدية لتجنب هجمات مماثلة حذر منها القراصنة، ويعني تعطيل خط الأنابيب حرمان ولايات الساحل الشرقي للولايات المتحدة من نصف كميات الوقود.

لم تكن شركة كولونيل بايبلين الوحيدة التي تعرضت للقرصنة واضطرت لدفع فدية. فقد دفعت شركة "جيه بي أس هولدنغ" الأمريكية ما يعادل ١١ مليون دولار من البيتكوين لقرصنة استهدفوا مصانعها لتصنيع اللحوم، وهددوا بتعطيلها عن العمل إذا لم تدفع الفدية.

وحسب مؤشر دارك تراكر، فقد جمع قرصنة داركسايد وحدهم ما يعادل نحو ٩٠ مليون دولار من عملة بيتكوين مؤخراً من عمليات قرصنة استهدفت ٩٩ شركة^(١). ويقدر المؤشر أن نحو نصف تلك الشركات دفعت الفدية كما طلب القراصنة. وتم تحويل العملة المشفرة إلى ٤٧ محفظة إلكترونية على شبكة بلوكتشين. لكن تلك المحافظ جرى تفريغها، ما يعني أن المجرمين حولوا الأموال إلى شركات صرافة وتداول العملات المشفرة، وغالباً، تختفي مجموعة القرصنة لتظهر أخرى باسم جديد وبرمجيات اختراق جديدة، وأيضاً بمحافظ رقمية جديدة لتحويل أموال الفدية إليها^(٢).

○ الفصل الثاني: التجربة اللبنانية مع العملات المشفرة

يحذر صندوق النقد الدولي وبنوك مركزية حول العالم ومنها مصرف لبنان من استخدام عملة بيتكوين والعملات المشفرة الأخرى. ورغم ذلك تظل سوق المشفرات كأصول رقمية متداولة ومغرية بالربح الكبير والسريع محل اهتمام المستخدمين، خصوصاً من الأجيال الجديدة التي دخلت الأسواق كمتعاملين. وأظهرت الأبحاث أن حوالي ثلث السكان فقط يمكنهم فهم البيانات والإحصائيات التي تشكل مخرجات حركة البيانات المفتوحة. تذهب تقنية البلوكتشين إلى أبعد من ذلك بكثير حيث تتطلب من المواطنين قبول نهج جديد تماماً لإدارة البيانات، وأن يكون لديهم بعض الفهم للتشفير ومبادئ الإدارة الرئيسية أو مواجهة خسارة أموالهم أو خدماتهم الحكومية. إن الانتقال إلى اقتصاد رقمي بالكامل دون تحديث أنظمتنا التعليمية هو وصفة كارثية مؤكدة.

^(١) <https://darktracer.com/>

^(٢) أحمد مصطفى، أي علاقة بين العملات المشفرة والقرصنة والجريمة المنظمة؟، ١١ حزيران ٢٠٢١ (أ ف ب) [/https://www.independentarabia.com/node/231091](https://www.independentarabia.com/node/231091)

وسنبحث في الفقرة الأولى تداول العملات المشفرة في لبنان، وفي الفقرة الثانية التشريعات المواكبة المطلوبة.

• الفقرة الأولى: تداول العملات المشفرة في لبنان

انهيار القطاع المصرفي في لبنان وامتنعت الدولة عن سداد ديونها منذ أوائل ٢٠٢٠، وفقدت الليرة اللبنانية قيمتها بشكل دراماتيكي في ثالث أسوأ انهيار اقتصادي منذ عام ١٨٥٠ بحسب البنك الدولي. ساهم التضخم الحاصل وانهيار العملة اللبنانية وخسارة الليرة أكثر من ٩٥% من قيمتها، وتآكل الرواتب وحجز المصارف لودائع اللبنانيين بالعملات الصعبة، في تفتيش الناس عن الاستثمار في العملات الرقمية للتخلص من فقدان القيمة. وسنعرض أولاً لتعدين العملات المشفرة، وثانياً التداول وسوق العملات المشفرة.

■ أولاً: تعدين العملات المشفرة

أضحى تداول العملات المشفرة سوقاً يستحق المجازفة عند اللبنانيين بعد انهيار الوضع المالي، وأفضل بكل حال من خسائر هائلة تكبدها المستخدمون والمودعون بالنظام المصرفي والاقتصادي. كل ذلك دفع إيجابياً باتجاه انشاء وتطوير مشاغل كانت موجودة (وتسمى مزارع) وتقوم بعمليات تعدين على نطاق واسع، وعلى الابتكار في مجال تعدين العملات الرقمية لتقديم قيمة بديلة في سياق انهيار الدولة، بما يتيح تأمين سبل العيش وتعزيز قدرة المجتمع على الصمود. وقد انتشرت في لبنان مشاغل تعدين العملات المشفرة والتي تستخدم كومبيوترات وأجهزة ذات مواصفات عالية وقادرة على إجراء عمليات حسابية معقدة، ولكن هذه الأجهزة بحاجة لكم هائل من التيار الكهربائي، والذي تُضاف فواتيره لكلفة التعدين مع ثمن الأجهزة. وتركزت المشاغل الخاصة في الأماكن التي تستفيد من موارد الطاقة المتجددة مثل الرياح والشمس والمياه كون موارد الطاقة الحرارية معدومة وإنقطاع شبه كامل بسبب غلاء البترول وفساد الإدارة في مؤسسة كهرباء لبنان. وتشمل عشرات الأماكن قرى تعتمد على الطاقة الكهرومائية في جبل لبنان أو الألواح الشمسية في البقاع وغيرها من الأماكن في العاصمة وضواحيها كون تشغيل المولدات لتعدين العملات الرقمية هي عملية غير مربحة.

وهناك ثلاثة أنواع من الأنشطة بالعملات الرقمية في لبنان:

"عمال التعدين" وينشط فيها أشخاص يقومون بإنشاء عملات جديدة وفك الشفرات وتتبع عمليات التداول عبر تسجيلها بسلاسل الكتل (Block chain)، بواسطة أجهزة كمبيوتر تتميز بكفاءة عالية مصممة لهذه الغاية، وتستهلك طاقة كهربائية ضخمة.^(١)

^(١) جنى الذهبي، مقال بعد انهيار الليرة والنظام المصرفي.. كيف تبدو وتيرة التداول بالعملات الرقمية في لبنان؟ تاريخ ٢٠٢١/١١/٢٢

موقع الجزيرة / <https://www.aljazeera.net/ebusiness/2021/11/22/>

"المؤثرون" والوكلاء المروجون (Influencers)، وهم الفئات التي تستثمر بالعملة الرقمية ويكون لديها رصيد خارجي ويلعبون دور الوسيط بتبادل الوحدات الرقمية. والمروجون ولديهم عناوين على وسائل التواصل الاجتماعي وقنوات على يوتيوب (YouTube)، وعلى تيك توك (TikTok)، ويعملون على التوعية عبر فيديوهات حول كيفية التحليل الفني للعملة الرقمية والمشاريع الأكثر تحقياً للأرباح. "المستخدمون" وهم مبتدئون ومستثمرون صغار وفئة كبيرة العدد نسبياً ولا تتعدى قيمة استثماراتهم بضع مئات من الدولارات.

وتعمل هذه الفئات في التجارة وتداول العملات الرقمية خارج إطار المنظومة المالية الرسمية، وتجري عمليات البيع والشراء على الشبكة السوداء والتي تنمو وتنتشر خاصة بين الشباب، وبالعملات المشفرة كونها آمنة ومن الصعب اختراقها أو تتبعها، وتزدهر أعمالهم في السوق السوداء الحقيقية، حيث تجري يومياً عمليات غير رقمية أيضاً كصرف الدولار والليرة وفقاً لسعر صرف السوق، ولا تمتلك المؤسسات المصرفية أي إشراف عليها^(١).

ويشكل تجار العملات الرقمية غير الشرعيين امتداداً لأنظمة الصرف غير الرسمية، التي يُشار إليها عادةً بشبكات الحوالة، والتي تقبل النقود وتحولها إلى عملة رقمية تُحفظ في محفظة رقمية، والعكس. والعملة المشفرة اقتصادياً اسمها "الموجودات الرقمية" ولا تملك مواصفات العملة، وشراؤها يتطلب توفر الدولار النقدي. ويوجد صرافان أليان لعملة البيتكوين في منطقة الحمراء في العاصمة بيروت لتحويل الدولار النقدي إلى بيتكوين، علماً بأن الصرافين الأليين يُستخدمان فقط في اتجاه واحد، أي إنه لا يمكن استعمالهما لسحب أوراق نقدية، ما يحد من أهميتهما عموماً للبنانيين العاديين الذين يجب أن يمتلكوا المعرفة التقنية للتداول بالعملة الرقمية بأنفسهم، أو أن يعتمدوا على شبكات تبادل شخصية.

أخيراً يحتاج لبنان إلى تمكين القدرة التنافسية للشركات الصغيرة والمتوسطة الحجم في مجال التكنولوجيا لاحتضان قدرات البيتكوين كقطاع اقتصادي مالي حديث. وتعتبر أهم تكلفة مرتبطة بتوليد كتل البيتكوين أي التعدين هي استهلاك الطاقة الكهربائية وهو السبب الذي جعل شركات التعدين تنشأ في مناطق تكون تكلفة الطاقة فيها منخفضة. تبقى البنية التحتية في لبنان متخلفة بشكل كبير في هذه الناحية، إلا أننا في حال ثبتت جدوى العملات الرقمية، فسوف نعول على الوعد بإنتاج النفط والغاز الذي يمكن أن يوفر فرصة لجذب الشركات التي تعمل في مجال العملة المشفرة^(٢).

^(١) متصفح TOR هو خاص للشبكة السوداء (Dark Web)، والأشهر بين المتصفحات الخاصة بتلك الشبكة، وقد بدأ مشروع البحرية الأمريكية للتواصل الآمن بين قطاعاتها والقيادة المركزية. يسمح المتصفح بالوصول السري إلى شبكة الإنترنت السوداء، مع ضمان عدم كشف الهوية أو الموقع الخاص بالمتصفح، ولا يحتاج تنبيته على جهاز الكمبيوتر سوى إلى تحميل الملف مجاناً من شبكة الإنترنت العادية.

^(٢) الوزير راند خوري، ندوة حول «البيتكوين» في الجامعة اللبنانية الألمانية، جريدة البناء - عدد الأربعاء ٣١ كانون الثاني ٢٠١٨. موجود أيضاً على موقع وزارة الاقتصاد [/https://www.economy.gov.lb/ar/press-releases/](https://www.economy.gov.lb/ar/press-releases/)

■ ثانياً: التداول وسوق العملات المشفرة

إن استخدام المنصات وتداول العملات ميسر وسهل بالعادة، وعلى سبيل المثال إن ما يتطلبه شراء العملة الرقمية USD Tether وبيعها مقابل الدولار في لبنان هو تنزيل تطبيق على الهاتف الخليوي وإدخال معلومات الاتصال بالشخص المعني لتسهيل التبادل^(١). وعززت فئات شبابية لبنانية استثماراتها بالعملات الرقمية، عبر الانضمام إلى مجموعات في واتساب (WhatsApp) أو تلغرام (Telegram)، حيث تجري معظم المعاملات الرقمية وهؤلاء من البارعين بمجال التكنولوجيا.

وفي المقابل إن منصات العملات الرقمية في لبنان غير مقننة وغير مشروعة، وهناك احتمال ولو نسبي أن تكون معرضة لعمليات احتيال ويصعب ملاحقة ومحاسبة مرتكبيها. وقد حذر حاكم مصرف لبنان عام ٢٠١٨ الجمهور من شراء العملات الرقمية ومنها البتكوين والتداول بها والذي اعتبرها مضاربة، مع تقلب شديد ليس له أي أساس اقتصادي ويكونها تشكل وسيلة هامة للمجرمين. وسبق أن حذر مصرف لبنان عام ٢٠١٤ من استخدام العملات الرقمية والذي وصفه بأنه مضاربة. ثم أصدر حاكم مصرف لبنان بصفته رئيس هيئة الأسواق المالية عام ٢٠١٨ حظراً على المؤسسات المالية المرخصة على إصدار نقودا إلكترونية ومنع تسويق العملات الرقمية أو التداول بها، لحسابها أو لحساب عملائها، بصورة مباشرة أو غير مباشرة، بما فيها المتداولة في الأسواق المالية المنظمة. ويحذر خبراء لبنانيون من الاستثمار العشوائي بالعملات الرقمية، استناداً إلى أنها مضاربة عالية المخاطر، ولأنها ليست بديلاً عن العملات ولا يوجد مؤسسات لبنانية تقبلها للتبادل النقدي، وغير موجودة بالتعريف التقليدي للعملة كوحدات متساوية قابلة للتبادل وحفظ القيمة^(٢). فالعملة الرقمية شديدة التقلب وفي حال وُجدت بكميات كبيرة قد تحمل مخاطر التأثير على الأسواق النقدية القائمة. لا يزال مجموع مخزون العملات الرقمية صغيراً نسبياً بحيث لا يشكل تهديداً، إلا أنه لا يمكن استبعاد مزيد من الزيادات وتفاقم حجم هذا المخزون ما قد يؤثر على الاستقرار المالي. ويعتقد الكثيرون في لبنان أن استثمار العملة العالم الرقمي سيصبح عنصراً أساسياً في المستقبل القريب، ومن المرجح أن يؤثر ذلك على ركائز عدة للاقتصاد بما في ذلك العملات، ولبنان بحاجة إلى الإعداد جيداً للعصر الرقمي من جميع النواحي.

ويُذكر هنا ان وجود مشاغل التعدين الكبيرة(المزارع) تسبب بضغط هائل على شبكة الكهرباء التي تُغذى من معامل التوليد الكهرومائية، مما تسبب بالكثير من الأعطال على الشبكة في تلك المناطق. هذا دفع بالمصلحة الوطنية لنهر الليطاني التقدم بكتاب رسمي في تشرين أول من العام ٢٠٢١ طلبت فيه من

(١) نيكولاس شافر، باحث في برنامج مارشال في جامعة أكسفورد ومعهد الدراسات الإنمائية، دراسة بعنوان تكشف عملية تعدين في جبال الشوف عن جاذبية العملات الرقمية في سياق الأزمة المالية في لبنان، ١٥ أيلول ٢٠٢٢ منشورة على الموقع <https://carnegieendowment.org/sada/87923>

(٢) مقال، بدلاً عن الدولار والذهب... لبنانيون يهرون بأموالهم إلى العملات الرقمية رغم المخاطر، ٢٤/١١/٢٠٢١

مؤسسة كهرباء لبنان، ووزارة الطاقة والمياه، ووزارة الداخلية والبلديات، والنيابة العامة التمييزية إزالة التعديلات والسرقات على شبكة التوزيع في منطقة القرعون ومشغرة⁽¹⁾. وفعلا داهمت الأجهزة الأمنية اللبنانية مطلع هذا العام العديد من مشاغل التعدين، في أكثر من قرية في البقاع الغربي، بالتنسيق مع هيئة أوجيهو ومؤسسة كهرباء لبنان، ولكن الأجهزة الأمنية ومن خلفها النيابة العامة لم تصدر أي شيء بل ساهمت في إزالة التعديلات على الشبكة وذلك لعدم وجود اي قانون ينظم التعدين او يمنعه، وانتقلت المشاغل الى مناطق اخرى.

• الفقرة الثانية: التشريعات المواكبة المطلوبة

يعتبر الإدماج المالي باستخدام العملات الرقمية المشفرة فرصة، وخصوصاً أنّ الأفراد والكيانات غير المصرفية أو التي لا تستخدم الخدمات المصرفية، بإمكانها الاستفادة من هذه التكنولوجيا الجديدة التي يعتبر الدخول إليها أسهل بكثير من الولوج إلى النظام النقدي التقليدي. كما من الممكن أن يستفيد منها الأفراد الذين يعانون من أزمات ومحن مثل اللاجئين الذين لا يحملون أوراق هوية أو لا توجد لديهم أي وثائق، أو البلدان التي تفنقر إلى بنية تحتية مصرفية راسخة ومنتشرة، حيث تكون فيها نسبة كبيرة من السكان غير قادرة على امتلاك حساب مصرفي.

ولكن النظام اللامركزي الذي يميز هذه العملات المشفرة يفنقر إلى الدقة والصلابة التي توفرها السلطات المركزية بحكم طبيعتها. ويبقى عدم وجود إطار تنظيمي وقانوني في العديد من السلطات القضائية يلقي بظلاله على حالة عدم اليقين بالنسبة للشركات ويجعل من الصعب على هذه العملات إثبات مصداقيتها وشرعيتها. ويزيد الحذر في الأعمال التجارية ومن قبل بعض المستهلكين من تلك العملات كونها لا تربطها أية علاقة بأي سلعة مادية مثل الذهب، وخصوصاً في غياب تشريعات توفر حماية المستهلك. وتحرص الدول على سن القوانين اللازمة والتي تواكب التوصيات الدولية، وكذلك العمل على استنباط الحلول والخلاصات وتشريع القوانين المرنة التي تلحظ المستقبل⁽²⁾.

وسنبحث أولاً في الاطار القانوني للعملات الرقمية في لبنان، وثانياً التشريعات المطلوبة.

■ أولاً: الإطار القانوني للعملات الرقمية في لبنان

تأثر لبنان بالتحوّلات الرقمية وتفاعل معها في كل الاتجاهات، وكانت تحضيرات جديّة من مصرف لبنان لإصدار عملة لبنانية رقمية مع نهاية عام ٢٠١٩ وحالت الظروف دون ذلك. وبعدها في كانون الثاني ٢٠٢٠ عدّل التعميم ٧٥٤٨ تاريخ ٢٠٠٠/٣/٣٠، وحظر إصدار النقود الإلكترونية من أي كان والتعامل

⁽¹⁾ محمد الصغير، ياسر الموسوي، مقال DARK WEB: الوجه المظلم للإنترنت السبت ٢٠ آب ٢٠٢٢ موجود على الموقع

<https://al-akhbar.com/Lebanon/343405>

⁽²⁾ <https://www.fatf-gafi.org/media/fatf/documents/brochuresannualreports/Annual-Report-2020-2021.pdf>

بها بأي شكل من الأشكال إلا وفقاً لاحكام القرارات الصادرة والتي ستصدر عن مصرف لبنان. علماً أن هناك عدداً من القوانين والأنظمة والتعاميم التي رعت الدفع والمعاملات الإلكترونية ومكافحة تبييض الأموال وتمويل الإرهاب وجرائم المعلوماتية كما يوجد مكاتب متخصصة بملاحقة هذه الجرائم⁽¹⁾. وسنبحث في بعض القوانين التي ترعى التحوّل الرقمي في لبنان.

١ - قانون المعاملات الإلكترونية والبيانات ذات الطابع الشخصي:

قُدّمت عدة مشاريع تتعلق بالدفع والاثبات الإلكتروني منذ ٢٠٠١ و٢٠٠٦ ومشروع ٢٠١٢ لقانون المعاملات الإلكترونية والبيانات ذات الطابع الشخصي رقم ٨١، والذي أقرّ عام ٢٠١٨. ويتمحور القانون حول الكتابة والتجارة والاثبات بالوسائل الإلكترونية والبيانات ذات الطابع الشخصي، ووردت احكام حول النقود الإلكترونية والرقمية في بعض نصوص هذا القانون. ويرى خبراء القانون أنه لم يذكر حرفياً العملات الرقمية الافتراضية والمشفرة خصوصاً من الناحية الجزائية، الأمر الذي يفسح المجال أمام المجرمين باقتراض الجرائم بواسطتها والإفلات من الملاحقة الجزائية نظراً لمبدأ شرعية الجرائم والعقوبات⁽²⁾.

وسبق أن حدّر مصرف لبنان عام ٢٠١٤ من استخدام العملات الرقمية والذي وصفه بأنه مضاربة. ثم أصدر حاكم مصرف لبنان بصفته رئيس هيئة الأسواق المالية عام ٢٠١٨ حظراً على المؤسسات المالية المرخصة على إصدار نقوداً إلكترونية ومنع تسويق العملات الرقمية أو التداول بها، لحسابها أو لحساب

⁽¹⁾ تمّ إنشاء مكتب مكافحة جرائم المعلوماتية وحماية الملكية الفكرية بموجب مذكرة الخدمة رقم ٢٠٤/٦٠٩ تاريخ ٢٠٠٦ آذار ٢٠٠٦ حيث أن موجبات انشاؤه كانت لمواكبة التطورات التكنولوجية والتقنية الحديثة في مجال المعلوماتية وبغية مكافحة الجرائم المتعلقة في مجال المعلوماتية وحماية لقطاع المعلوماتية في لبنان. ثم صدر تعميم من النيابة العامة التمييزية رقم ٧٢/ص/٢٠١٣ تاريخ ٧ حزيران ٢٠١٣ طلبت فيه من النيابة العامة إحالة الشكاوى والاستنسابات القضائية التي تدخل ضمن صلاحيات مكتب مكافحة الجرائم المعلوماتية وحماية الملكية الفكرية وفقاً لما يلي

1. مكافحة الجرائم المعلوماتية لا سيما التعديّات التي تقع على أنظمة المعلوماتية وشبكاتها وخوادمها، وعلى المواقع الإلكترونية لا سيما تعطيلها عن العمل أو إعادة تحويل المستخدمين إلى مواقع زائفة، وما يرتبط بها من تعديّات على البيانات، وتخزينها وحفظها، واعتراض انتقالها، والقرصنة، وصناعة ونشر فيروسات.

2. مكافحة الجرائم التي ترتكب بواسطة أجهزة المعلوماتية كوسيلة مساعدة الارتكاب الجرائم الأصلية، مثل التهديد والابتزاز وتشويه السمعة والقدح والدّم وانتحال الصفة والتحرّش والاحتيال الإلكتروني.

3. عند تحقق المكتب من جرائم تدخّل في اختصاصات المكاتب الأخرى ذات الاختصاص النوعي مثل المخدرات والقمار والجرائم المالية والإرهاب والآداب والسرقات الدولية وغيرها، فإنّ المكتب المذكور، ينظّم محضراً بالواقع بناءً لإشارة القضاء المختص ويضمنه كافة المعلومات ويحيلها إلى المكتب المختص لإستكمال إجراءات التحقيق والملاحقة.

4. مكافحة الجرائم المنصوص عنها في القانون رقم ٧٥/٣ تاريخ ١٩٩٤/٤/٣ الرامي إلى حماية الملكية الأدبية والفنية.

٥. مكافحة الجرائم الواقعة على التطبيقات الذكية Apps والتطبيقات والمواقع المشبوهة ومكافحة الجرائم الواقعة على الإقتصاد الرقمي.

⁽²⁾ ماريلين أوردكيان، العملات الافتراضية المشفرة في الحقل الجنائي السيبراني، لعدد ١٠٨ - نيسان ٢٠١٩

عاملها، بصورة مباشرة أو غير مباشرة، بما فيها المتداولة في الأسواق المالية المنظمة. في حين حذر الجمهور من شراء العملات الرقمية ومنها البتكوين والتداول بها بكونها تشكل وسيلة هامة للمجرمين^(١).

تضمنت المادة الأولى من القانون رقم ٢٠١٨/٨١ تعريفاً للنقود الإلكترونية والرقمية كما يلي: النقود الإلكترونية والرقمية (Monnaie Électronique et numérique/Digital or Electronic Money): هي وحدات تسمى وحدات نقد إلكتروني يمكن حفظها على دعامة إلكترونية. تشمل العملات الرقمية النقود الإلكترونية والعملات الافتراضية^(٢). فالأولى أي النقود الإلكترونية، والتي نصت عليها المادة الأولى من قانون ٢٠١٨/٨١، شملتها عدة قوانين ومنها التوجيه الأوروبي رقم ٢٠٠٩/١١٠/EC وتعني النقود الورقية كاليورو والتي تُستعمل في المعاملات والتجارة الإلكترونية، وهذه النقود لا تمت بأي صلة بالعملات الافتراضية والمشفرة. أما العبارة الثانية أي العملات الافتراضية، فتعني بحسب التوجيه الأوروبي رقم ٨٤٣/٢٠١٨ تمثيلاً رقمياً لقيمة معينة، فهي الأموال الموجودة فقط بنموذج رقمي ولا تتمتع قانوناً بصفة نقود ولا تصدر عن مصرف مركزي أو سلطة عامة، وتدخل العملات المشفرة بفئة العملات الافتراضية هذه^(٣). ونصت المادة ٦١ من القانون ٢٠١٨/٨١ على أن تحدد الأنظمة الصادرة عن مصرف لبنان ماهية النقود الإلكترونية والرقمية وكيفية إصدارها واستعمالها والتقنيات والأنظمة التي ترعاها.

ويمكن تعداد الجرائم المتعلقة بالمعاملات الإلكترونية والبيانات ذات الطابع الشخصي والتي نصّ عليها القانون ٨١ في الفصل الخامس منه كالتالي:

أ. الجرائم المتعلقة بالأنظمة والبيانات المعلوماتية ويمكن تعداد هذه الجرائم كالتالي: الولوج غير مشروع إلى نظام معلوماتي، والتعدي على سلامة نظام المعلوماتي، والتعدي على سلامة البيانات الرقمية، وإعاقة أو تشويش أو تعطيل الوصول إلى خدمة إلكترونية، إساءة التصرف بالأجهزة والبرامج المعلوماتية، والتزوير الإلكتروني^(٤).

ب. الجرائم المتعلقة بالأنظمة والبيانات المعلوماتية والبطاقات المصرفية^(٥).

ج. جريمة تقليد بطاقة الدفع أو السحب المصرفية وتزويرها وحدد القانون كل من:

- قلد بطاقة مصرفية أو زورها
- استعمل أو تداول، مع علمه بالأمر بطاقة مصرفية مزورة أو مقلدة.
- قلد نقوداً إلكترونية أو رقمية
- استعمل، مع علمه بالأمر نقوداً إلكترونية أو رقمية مقلدة.

(١) مصرف لبنان، هيئة الأسواق المالية، إعلام رقم ٣٠ تاريخ ٢٠١٨/٢/١٢

(٢) FATF, Virtual Currencies Key Definitions and Potential AML/CFT Risks , Ibid

(٣) Council of Europe: Directive 843/2018, p.54, Ibid

(٤) عدّل القانون ٨١ نص المادة ٤٥٣ من قانون العقوبات اللبناني حول التزوير الإلكتروني. واصبحت كالتالي: "التزوير هو تحريف متعمد للحقيقة في الوقائع أو البيانات التي يثبتها صك أو مخطوط أو دعامة ورقية

أو إلكترونية أو أية دعامة أخرى للتعبير بشكل مستقداً، بدافع إحداث ضرر مادي أو معنوي أو إجتماعي".

(٥) تعديلات على قانون العقوبات وقواعد إجرائية متعلقة بضبط الألة المعلوماتية وحفظها، القانون ٨١ تاريخ ٢٠١٨/١٠/١٠ المعاملات الإلكترونية والبيانات ذات الطابع الشخصي.

- قَدَّ شيكاً إلكترونياً أو رقمياً.
- استعمل مع علمه بالأمر، شيكاً إلكترونياً أو رقمياً مقلداً.

٢- قانون الحق في الوصول إلى المعلومات رقم ٢٠١٧/٢٨

يُعدّ أول قانون يتناول صراحة البيانات والمعلومات، إنّما ضمن إطار محصور بتلك المتوفرة لدى أجهزة القطاع العام وإداراته كافة (مع وجود الاستثناءات)، كانت الحاجة ملحة لقانون يختص بالبيانات الرقمية الشخصية كافة. وهنا تكمن أهمية القانون رقم ٨١/٢٠١٨، الذي يضع بدوره الأسس والقواعد التنظيمية من ناحية تجميع البيانات ذات الطابع الشخصي ومعالجتها واستخدامها.

٣- قانون النقد والتسليف ١٩٦٣

أعطى القانون مصرف لبنان حق إصدار الأنظمة اللازمة المتعلقة بتنظيم أوامر الدفع والنقود الإلكترونية والرقمية والتحويلات والشيكات الإلكترونية والصورة الرقمية للشيك والتمثيل الرقمي للشيك والشيك الرقمي، وكيفية إصدارها واستعمالها، وأصول حفظ القيود المصرفية ومدة حفظها بالإضافة إلى وسائل الحماية والأمان اللازمة. هذه المرونة في العمل وتلك الصلاحيات تتمثل بأشرف المصرف المركزي على السياسة المالية. وأصدر المصرف المركزي عدداً من التعميمات أهمها ٨٣٤١ تاريخ ٢٤/١/٢٠٠٣ و٧٥٤٨ تاريخ ٣٠/٣/٢٠٠٠ وتعديلاته كانون الثاني ٢٠٢٠، وحظر المصرف المركزي في هذا التعميم إصدار النقود الإلكترونية من أي كان والتعامل بها بأي شكل من الأشكال الا وفقاً لاحكام القرارات الصادرة والتي ستصدر عن مصرف لبنان. وذكرنا أن مصرف لبنان ومنذ عام ٢٠١٤ حدّر من استخدام العملات الرقمية والذي وصفه بأنه مضاربة وحدّر الجمهور من شراء العملات الرقمية ومنها البتكوين والتداول بها بكونها تشكل وسيلة هامة للمجرمين. وقد أصدر حاكم مصرف لبنان بصفته رئيس هيئة الأسواق المالية عام ٢٠١٨ حظراً على المؤسسات المالية المرخصة على إصدار نقوداً إلكترونية ومنع تسويق العملات الرقمية أو التداول بها، لحسابها أو لحساب عملائها، بصورة مباشرة أو غير مباشرة، بما فيها المتداولة في الأسواق المالية المنظمة. وكان أكد حاكم مصرف لبنان مراراً قبل عام ٢٠٢٠ على مشروع إصدار عملة رقمية محلية من قبل المصرف المركزي ولكن المشروع لم يبصر النور.

٤- قانون ٢٠١٥/٤٤ المتعلق بهيئة التحقيق الخاصة

نشأت هيئة التحقيق الخاصة بموجب القانون رقم ٢٠٠١/٣١٨ المعدل بموجب القانون ٢٠١٥/٤٤، وهي هيئة مستقلة داخل المصرف المركزي، ذات طابع قضائي، وتتمتع بالشخصية المعنوية، وغير خاضعة

في ممارسة أعمالها لسلطة مصرف لبنان^(١). وتتعدد مهام الهيئة ولا يعتد أمامها بالسرية المصرفية، ولا تقبل قراراتها أي طريق من طرق المراجعة العادية وغير العادية الإدارية أو القضائية بما في ذلك المراجعة لتجاوز حد السلطة^(٢). وتتشكل الهيئة من حاكم مصرف لبنان رئيساً، ورئيس لجنة الرقابة على المصارف، والقاضي المعين في الهيئة المصرفية العليا، وعضو يعينه مجلس الوزراء بناءً على اقتراح من حاكم مصرف لبنان^(٣). تعرف هيئة التحقيق الخاصة (SIC) عن نفسها بأنها وحدة استخبارات مالية متعددة الوظائف (FIU) ذات وضع قضائي. وتشكل الجزء الأساسي من نظام مكافحة غسل الأموال وتمويل الإرهاب في لبنان، ومنصة للتعاون الدولي، ومن المفترض أن تلعب دوراً حيوياً في حماية القطاعات المعنية من العائدات غير المشروعة وتشمل عائدات الفساد، بما في ذلك الرشوة وصرف النفوذ والاختلاس واستثمار الوظيفة وإساءة استعمال السلطة والإثراء غير المشروع^(٤). وقد بدأت هيئة التحقيق الخاصة بتنفيذ مهامها في أيلول ٢٠٠١، ونالت الثقة من الدول الخارجية^(٥). كما أصدر مصرف لبنان تعميم رقم ٢٠٠١/١٩١٢ الصادر بتاريخ ٢٠٠١/٥/١٨ المتعلق بنظام مراقبة العمليات المالية والمصرفية لمكافحة تبييض الأموال. وبتاريخ ٢٣ تموز ٢٠٠٣ أصبح لبنان عضواً في مجموعة إغمونت Egmont الدولية لمكافحة تبييض الأموال، ولعب أيضاً دوراً أساسياً في إنشاء مجموعة المينافاتف عام ٢٠٠٤ (MENAFATF) وتولى رئاستها في السنة الأولى^(٦). كما تم إنشاء نظم إلكترونية لتبادل المعلومات مع الأجهزة المختصة وذلك لمكافحة جرائم تبييض الأموال بشكل أكثر فعالية^(٧). وقد أكد القانون ٢٠١٥/٤٤ تاريخ ٢٠١٥/١١/٢٤ على الإجازة للحكومة اللبنانية الانضمام إلى الإتفاقية الدولية لقمع تمويل الإرهاب الموقعة في نيويورك بتاريخ ١٩٩٩/١٢/٩. وقد

(١) الجريدة الرسمية ٢٠١٥، عدد ٤٨، قانون رقم ٤٤/٤٤ تاريخ ٢٠١٥/١١/٢٤، مكافحة تبييض الأموال وتمويل الإرهاب، ص ٣٣١٥.

(٢) الخوري، جنان، تبييض الأموال الجريمة الجزائية المصرفية والتبعية، مجلة الجيش، عدد ٨٢، ٢٠١٣.

(٣) نصت المادة ٦ من قانون ٢٠١٥/٤٤ تنشأ لدى مصرف لبنان هيئة مستقلة، ذات طابع قضائي، تتمتع بالشخصية المعنوية، غير خاضعة في ممارسة أعمالها لسلطة المصرف وتسمى فيما يلي «هيئة التحقيق الخاصة» أو «الهيئة» وتتألف «هيئة التحقيق الخاصة» من: حاكم مصرف لبنان وفي حال تعذر حضوره، من ينتدبه من بين نوابه - رئيساً.

القاضي المعين في الهيئة المصرفية العليا، وفي حال تعذر حضوره، قاض رديف يعينه مجلس القضاء الاعلى لمدة تعادل مدة تعيين القاضي الاصيل - عضواً.

رئيس لجنة الرقابة على المصارف، وفي حال تعذر حضوره، من ينتدبه من بين اعضاء اللجنة المذكورة - عضواً.

عضو اصيل وعضو رديف يعينهما مجلس الوزراء بناءً على إهاء حاكم مصرف لبنان، على ان تتوفر فيهما خبرة لا تقل عن ١٥ سنة في مجال القانون المالي او المصرفي - عضواً.

(٤) المادة الاولى فقرة ٩ من قانون ٢٠١٥/٤٤

(٥) هيئة التحقيق الخاصة، التقرير السنوي، ٢٠٢٠ على موقع الهيئة

<https://sic.gov.lb/sites/default/files/publications/SIC%20Annual%20report%202020%20Arabic.pdf>

(٦) تقرير مجموعة العمل المالي لمنطقة الشرق الأوسط وشمال أفريقيا من أجل مكافحة غسل الأموال وتمويل

الإرهاب، ٢٠١٥/٦/٢٠ www.menafatf.org

(٧) هيئة التحقيق الخاصة، التقرير السنوي، ٢٠٢٠ مرجع سابق .

أضيف إلى مهامها موضوع مكافحة الفساد بموجب القانون ٢٠٠٨/٣٢ تاريخ ٢٠٠٨/١٠/١٦ تطبيقاً لاتفاقية الامم المتحدة لمكافحة الفساد.

أعطيت هيئة التحقيق الخاصة صلاحية هائلة بموجب القانون ٢٠١٥/٤٤ للقيام بمهام متعددة منها تلقي البلاغات وطلبات المساعدة، وإجراء التحقيقات والاطلاع على الحسابات المصرفية، من دون أن تكون ملزمة بالسرية المصرفية ولها حق رفعها بالكامل^(١). كما لها صلاحية إجراء تجميد احترازي أو نهائي للحسابات المصرفية، وإبقاء الحسابات المشتبه بها قيد المتابعة، وجمع وحفظ المعلومات الواردة من المعنيين. ويمكن للهيئة التحرك من تلقاء ذاتها وتلقي البلاغات وطلبات المساعدة وإجراء التحقيقات في ما يشتهه أن يكون عمليات مشبوهة أو تبييض أموال. واستجابت السلطات اللبنانية المعنية إلى طلبات المعلومات والبلاغات الاجنبية فوراً دون الاعتداد تجاه الهيئة بأي موجب للسرية^(٢).

وأعطيت الهيئة بموجب قانون نقل الأموال عبر الحدود ٢٠١٥/٤٢ تاريخ ٢٠١٥/١١/٢٤ صلاحية الاطلاع على التحقيق حول الأموال المنقولة والتي لم يصرح عنها للجمارك أو مشتبه بها عبر الحدود. كما أعطيت بموجب القانون ٢٠١٦/٥٥ تاريخ ٢٠١٦/١٠/٢٧ في مادته الوحيدة في البند سادساً صلاحية رفع السرية عند كل طلب لتبادل المعلومات الضريبية خاصة مع الدول التي يرتبط معها لبنان باتفاقيات تبادل المعلومات^(٣).

وأعطى القانون رقم ١٧٥ / ٢٠٢٠ / ٨ تاريخ ٢٠٢٠ / ٥ / ٨ المتعلق بمكافحة الفساد في القطاع العام وإنشاء الهيئة الوطنية لمكافحة الفساد في المواد ١٩ و ٢٠ الاطار العملي للتعاون مع هيئة التحقيق الخاصة في اطار ملاحقة الفساد واتخاذ الاجراءات.

وهناك العديد من تعاميم مصرف لبنان التي تحدد دور الهيئة في تطبيق القوانين وصلاحياتها الهائلة في كل المجالات وعلى جميع المؤسسات في لبنان^(١).

(١) المادة السادسة من القانون ٢٠١٥/٤٤

(٢) نصت المادة الثانية من قانون ٢٠١٥/٤٤ إن جريمة تبييض الأموال هي جريمة مستقلة ولا تستلزم الإدانة بجرم أصلي، كما أن إدانة الفاعل بالجرم الأصلي لا يحول دون ملاحقته بجرم تبييض الأموال في حال وجود اختلاف بالعناصر الجرمية. يعتبر تبييض أموال كل فعل يقصد منه:

١- إخفاء المصدر الحقيقي للأموال غير المشروعة أو إعطاء تبرير كاذب لهذا المصدر، بأي وسيلة كانت، مع العلم بأن الأموال موضوع الفعل غير مشروعة.

٢- تحويل الأموال أو نقلها، أو استبدالها أو توظيفها لشراء أموال منقولة أو غير منقولة أو للقيام بعمليات مالية بغرض إخفاء أو تمويه مصدرها غير المشروع أو بقصد مساعدة أي شخص متورط في ارتكاب أي من الجرائم المنصوص عنها في المادة الأولى على الإفلات من الملاحقة مع العلم بأن الأموال موضوع الفعل غير مشروعة. ونصت المادة الأولى البند

٧- استغلال المعلومات المميزة وافتشاء الأسرار وعرقلة حرية البيوع بالمزيدة والمضاربات غير المشروعة

٩- الفساد بما في ذلك الرشوة وصرف النفوذ والاختلاس واستثمار الوظيفة وإساءة استعمال السلطة والإثراء غير المشروع.

(٣) هيئة التحقيق الخاصة، التقرير السنوي، ٢٠٢٠ على موقع الهيئة، ص ٧٨

<https://sic.gov.lb/sites/default/files/publications/SIC%20Annual%20report%202020%20Arabic.pdf>

إن تمتع هيئة التحقيق الخاصة بكل هذه الصلاحيات وعدم استخدامها إلا لمصالح خاصة أجنبية وغب الطلب محليا واستتسابيا، واحجامها عن دورها عند حاجة اللبنانيين اليها، ووصول الوضع المالي الى ما وصل اليه في لبنان، وفشلها الذريع في أداء ما أنشئت من أجله استدعت النظر جديا بمسألة وجودها أصلا لزوم ما لا يلزم. وهناك مشروع قانون لتعديل الهيئة وتوسعة ادارتها، ولكن تعدد الهيئات وتعدد المصاريف وتعدد الصلاحيات، وتراكم البيروقراطية لا تحقق العدالة فالمطلوب الشفافية وتطبيق القانون. وهناك اقتراح تفعيلها نظرا لاهميتها وذلك عبر ضمها ونقل صلاحياتها إلى الهيئة الوطنية لمكافحة الفساد التي أنشأت بموجب القانون ٢٠٢٠/١٧٥ وتكون بمثابة وحدة استقصاء مالي داخلها ما يحقق الحوكمة الرشيدة لهذه الوحدة والاستقلالية فعلاً لا قولاً وتحقيق الهدف من وجودها^(٢).

■ ثانياً: التشريعات المطلوبة

١- الإستثمار في اقتصاد رقمي يصل للجميع

أضيفت إلى الحقائق الوزارية في الحكومة اللبنانية بداية عام ٢٠١٩ وزارة جديدة، هي وزارة الدولة لشؤون الاستثمار والتكنولوجيا، التي أسندت إلى الوزير عادل أفيوني. وقد ساهم في تحويل التعهد الذي أعلنته الحكومة في بيانها الوزاري بالتحوّل نحو الاقتصاد الرقمي إلى واقع مع خطة لمحو الامية الرقمية. كما حقق إقرار بندين في موازنة العام ٢٠١٩ لدعم حوافز وتشجيع التوظيف في قطاع اقتصاد المعرفة، لكن الوقت لم يسعفه حيث استقالت حكومة الحريري بعد ثورة ١٧ تشرين ٢٠١٩، ولم تأت حكومة الرئيس حسان دياب المشكّلة بتاريخ ٢١ كانون الثاني ٢٠٢٠ على ذكرها وكذلك تجاهلتها حكومة الرئيس ميقاتي الحالية التي تشكلت عام ٢٠٢١. وعمل الوزير على المراسيم التطبيقية لقانون المعاملات الإلكترونية والبيانات ذات الطابع الشخصي رقم ٢٠١٨/٨١، ومنها مرسوم لتنظيم الإجراءات الخاصّة والضمانات المتعلقة بالأسناد الرسمية، ونطاقها الوارد في المادة الثامنة منه^(٣)، ومرسوم يحدّد آلية حفظ المعلومات المتعلقة بحركة البيانات، وماهيّة هذه المعلومات من قبل مقدّمي الخدمات التقنية الوارد بالمادة اثنتان وسبعون، وتألّف الهيئة الوطنية لإدارة النطاقات الخاصّة بلبنان الواردة بالمادة تسعة وسبعون من نفس القانون. ولذا يجب متابعة هذا العمل للوصول إلى الاقتصاد الرقمي. وعليه لا بد من الالتزام بوزارة الدولة لشؤون الاستثمار والتكنولوجيا اسوة بكل الدول التي تسعى إلى المستقبل كالامارات العربية مثلا التي اعتمدت وزارة للذكاء الاصطناعي.

(١) هيئة التحقيق الخاصة، التقرير السنوي، ٢٠٢٠ على موقع الهيئة، ص ٧٨

<https://sic.gov.lb/sites/default/files/publications/SIC%20Annual%20report%202020%20Arabic.pdf>

(٢) زهير بشناق، هيئة التحقيق الخاصة ومصيرها، مقال مجلة house of law gazette، العدد ٢، تموز ٢٠٢٢.

(٣) قانون رقم ٨١/٨ المعاملات الإلكترونية والبيانات ذات الطابع الشخصي ١٠ تشرين الاول ٢٠١٨

٢- الهوية الرقمية

تستخدم جوازات السفر في لبنان ورخص القيادة وإجازات العمل والإقامة والمساعدات الإنسانية على أنواعها أنظمة قائمة على البيانات البيومترية، كبصمات الأصابع وبصمة العين، وهي بيانات تجمعها الدولة من اللبنانيين والمقيمين في لبنان. نصّ قانون الانتخابات عام ٢٠١٧ على استخدام الناخبين لبطاقات إلكترونية ممغنطة أو الهوية الرقمية. لم تتحقّق الخطط الرامية إلى اعتماد الهوية البيومترية قبل الموعد المحدّد للانتخابات النيابية في العام ٢٠١٨ ولم تتحقّق أيضا في انتخابات ٢٠٢٢ ولغاية اليوم، ولكن لمح التعديل الصادر عن مجلس الوزراء إلى رغبة الحكومة ببناء نظام هوية وطني يربط الهوية البيومترية بعملية تقديم الخدمات. وفي ظلّ الأزمة الإقتصادية التي يواجهها لبنان هناك توجّه إلى الشروع في تطبيق برنامج الهوية الرقمية للتحقّق من الهويات والمصادقة عليها، لا سيّما في سبيل دعم برامج شبكة الأمان الاجتماعي الممولة من البنك الدولي.

٣- خطة التحوّل الرقمي

قدّمت وزارة الدولة لشؤون التنمية الإدارية OMSAR استراتيجية التحوّل الرقمي الشاملة عام ٢٠١٨ بعد أكثر من خمس وعشرين عاما من العمل. وضعت خطة التحوّل الرقمي لعشر سنوات ٢٠٢٠-٢٠٣٠ ونُشرت بعضها على موقع الوزارة الإلكتروني. نفذت الوزارة عشرات المشاريع الناجحة خلال هذه المدة في مختلف الوزارات والمؤسسات وهي ممولة خارجيا من الاتحاد الاوروبي والبنك الدولي وجهات مانحة دولية. ويهدف موقع "دولتي" الإلكتروني وهو الأهم إلى إرساء مدخل للحكومة الإلكترونية، حيث يتجمع في الموقع كافة الوزارات والمؤسسات العامة بغية توحيد خدماتها الإلكترونية. يوفر الموقع للمؤسسات خدمات رقمية أساسية مثل منصة التبادل المعلوماتي، وتقنية المصادقة على الهوية، والمعاملات الإلكترونية، وتطبيقا لتتبع سير العمليات وغيرها. ونفذت الوزارة مشروع منصة التسجيل في السجلّ التجاري الإلكترونية وربط عددا من الوزارات المعنية، واتاحت المنصة التبادل الإلكتروني للبيانات. وتعتبر هذه المشاريع بداية ترتيب للحكومة الإلكترونية المرتقبة. ويلاحظ المراقبون البطء في انجاز المشاريع وعلو تكلفتها التي تجاوزت ٨٠ مليون دولار نتيجة تحكّم البيروقراطية والفساد والأمية الرقمية احيانا في كثير من المواقع التي تعمل على تعقيد الاجراءات بدل تبسيطها لتوحيدها وجمعها لزوم البرامج الإلكترونية.

وفي نيسان ٢٠٢٠ أعلن النفتيش المركزي عن إطلاق منصة البلديات المشتركة للتقييم والتنسيق والمتابعة وهو مشروع يدعم التوجه نحو حكومة إلكترونية في لبنان. واستفادت وزارة الداخلية والبلديات من هذه المنصة في مواجهة فيروس كورونا وإدارة الازمة والتنسيق عام ٢٠٢١ كما استفادت وزارة الشؤون الاجتماعية منها عام ٢٠٢٢ في اطار احصاءات الاسر الاكثر فقرا .

ولكن لبنان انتقل بموجب مؤشر التوجهات العالمية للحكومة الإلكترونية ضمن دراسة لجنة إدارة الشؤون الإقتصادية والاجتماعية في الامم المتحدة لعام ٢٠٢٠ من مرتفع إلى متوسط للحكومة الإلكترونية، اي

تراجع من الدرجة الثانية إلى الدرجة الثالثة قبل الأخيرة وهي علامة بين ٢٥-٥٠. وفي نفس الدرجة في مؤشر الخدمات عبر الإنترنت وترتيبه ١٢٧، وصنّف من بين الدول الأقل اتصالاً في العالم، مع المعدلات الأقل لاختراق النطاق العريض هو ١%. وأتى ترتيبه ١٤٨ من ١٩٣ دولة بالنسبة إلى حجم المشاركة على الإنترنت^(١).

٤- استراتيجية الأمن السيبراني

الأمن السيبراني ليس متحققاً في كافة أنظمة المعلومات في لبنان إلا في دوائر أمنية ضيقة. وتعاني العديد من المؤسسات في القطاعين العام والخاص من عدم قدرة على رد الهجمات الداخلية والخارجية السيبرانية التي تجتاحها وتعطل عملها. إستدعى ذلك تشكيل هيئة لتحقيق استراتيجية بتكليف من رئيس الوزراء بموجب قرار رقم ١٧٣ بتاريخ ٢٦/٩/٢٠١٨. أصدرت الهيئة المؤلفة من ١٥ عضواً يمثلون المؤسسات الأمنية، والوزارات المعنية، ومصرف لبنان، وعلى رأسها الأمين العام للمجلس الأعلى للدفاع منشوراً في حزيران ٢٠١٩ حول الاستراتيجية الوطنية للأمن السيبراني نحو عام ٢٠٢٢، وتهدف إلى فضاء سيبراني أكثر أماناً. تشمل الحماية الدوائر الحكومية والتجارة الإلكترونية والشركات والأفراد من الهجوم السيبراني، وكل أشكال القرصنة، أو العبث بالمحتوى، والإرهاب وغير ذلك من المخاطر. طالبت الهيئة بإنشاء ودعم "الوكالة الوطنية للأمن ونظم المعلومات" تعمل بإشراف المجلس الأعلى للدفاع ويكون لديها فريق عمل للتدخل والحماية. إن تطوير الأمن السيبراني وقدرات المعرفة الرقمية الأوسع يجب أن تمكن مستخدمي الحكومة الإلكترونية، بما في ذلك المجموعات الضعيفة، لتصبح أكثر أماناً عبر الإنترنت، للمطالبة بأمان البيانات وحماية السلامة، وللدفاع عن أنفسهم ضد التهديدات المتنوعة^(٢).

٥- تغيير نمط القوانين

تتعَدّل وتتغيّر القوانين مع تطوّر المجتمعات منذ القدم وفق السياق التاريخي، ولا يوجد مجتمع دون قوانين وأدوات ضبط معتمدة. فعند انتقال المجتمعات سياسياً أو اقتصادياً من مرحلة إلى أخرى أو عند بروز تداعيات الثورات الصناعية توقف العدل في مرفق العدالة، وإهتَزّ الضبط الإجتماعي لفترة طالت أو قصرت بحسب قوة الدولة وتنظيمها، وبعُد نظر النخب الفاعلة وقدرتها على المواجهة. أثناء ذلك تعمل أدوات الضبط العدلية والشرطية بالأدوات القديمة، والأمثال كثيرة حيث يتم رفض كل جديد. ينتج عن الممارسات الجديدة سقوط النظام القانوني القديم لعدم صلاحيته وعجز أدوات الضبط أمام التحدّي والتحديث. وهذا ما يحدث اليوم

^(١) دراسة موجودة على الموقع

<https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2020>

^(٢) الاستراتيجية الوطنية للأمن السيبراني، رئاسة مجلس الوزراء حزيران ٢٠١٩ (pdf) موجودة على الموقع

<http://www.pcm.gov.lb/arabic/subpg.aspx?pageid=13537>

في الثورة الرقمية. ففي خضم السرعة الفائقة في التغيير التقني وانتقال الاطفال من متلقين إلى فاعلين وعصر الجيل الخامس حيث الآلة مسؤولة عن اتخاذ القرارات بنفسها، وتحمل مسؤولية الفعل الضار الذي لم يعلم به مشغلها، وسيكون الفاعل في أغلب الاحيان أجنبي ولا وصول له والضحية مواطن ويصح القول ضبطنا القتل وهرب القاتل.

لذلك لا بد من تغيير النمط في التحرك القانوني ليوافق السرعة وتشكيل قوانين أطر والتخلي عن القوالب الجامدة للقوانين الرقمية التي تشكل فحاً لكل مواطن صالح حسن النية أخطأ بشكل عرضي فقط. أما انتهازيو الشبكة وأصحاب الأفكار الجرمية وشركات الأمر والنهي على الانترنت والشبكة السوداء فهم في مأمّن وشبكاتهم أكبر من بلادنا العربية. واعطي مثلا عن العجز عن محاسبة شركة فايسبوك عن انتهاك خصوصية المستخدمين.

ومن هنا ضرورة وضع القوانين الأطر واعتماد المراسيم والنظم المتحركة، والإعتماد على الاجتهاد والمحاكم واعتماد القضية المحكوم بها في الفضاء السيبراني، والتي يمكنها مواكبة ما يستجد. وأعطي مثلاً عن تعديل قاعدة مكرّسة أن لا جريمة دون نص ولا عقوبة دون نص، حيث يمكن التجريم، وتكون العقوبة الأولى تنبيه خطي من سلطات الملاحقة على أن يكون هناك تعديل على النظام الحامي بعد إحالة الفعل الضار أو الجرم إلى النيابة العامة الإلكترونية وحجب الموقع، والتي تحيله إلى نظام يعاقب عليه بعد نشره بعشرة أيام.

وعليه، لا بد من تشريع قانون جديد للفضاء الإلكتروني يدمج كل القوانين ويكون الإطار العام، وتغيير القوالب من جامدة إلى متحركة ليغطي كل المستجدات والتصرفات. ويحتوي القانون على أصول المحاكمات وإستحداث نيابة عامة ومحاكم رقمية للفضاء السيبراني كاملة ومحكمين رقميين وتكليف قضاة الاساس بالأحكام وفق القانون وما تمليه الضمانات.

○ الخاتمة

تُرْتَكَب أغلب جرائم الإنترنت على أيدي القراصنة وهم لصوص يودون تغيير واقعهم أو كسب الأموال، أو تبييض أموال غير مشروعة أو تمويل إرهاب عبر الدول دون المرور بالحدود الجغرافية، وأحياناً نادرة أخرى يكون الهدف من وراء جرائم الإنترنت هو إلحاق الضرر بالافراد أو الهيئات أو بأجهزة الكمبيوتر لأسباب غير الربح، وقد تكون هذه الأسباب سياسية أو شخصية. وقد وجد المجرمون العملة المشفرة وسيلة واداة فاعلة للتداول نظرا لطبيعتها وتحقيق الجرائم الإلكترونية وتسيير النشاط الإجرامي كما أنها أصبحت هي نفسها محل استهداف المجرمين ومحل الجرائم.

وتعتبر المركزية والسيطرة الحكومية ومعرفة هوية المستخدمين، من أهم العوامل لاعتماد العملات الرقمية والمشفرة، حيث إن الدول تكون معها قادرة على أن تكون المصدر المركزي الرئيسي والمنظم

لاستخدامها ووضع ضريبة على الأرباح، كما أن ذلك يجعلها قادرة على التصدي لأي استخدامات غير قانونية أو إجرامية لتبييض الأموال وتمويل الإرهاب.

وتستخدم العملات الرقمية في جرائم الانترنت وكذلك خارج الفضاء السيبراني مثل غسل الأموال وتمويل الإرهاب والاتجار بالبشر وجمع البيانات الرقمية بطريقة غير شرعية أو من دون تصريح، وإساءة استخدامها من قبل الحائز، والولوج إلى نظام معلوماتي والإقدام على نسخها، تعديلها أو إلغائها، والتعدي على سرّيتها عن طريق نشرها، تسريبها، إفشائها لأشخاص غير مخولين الاطلاع عليها. أما العلاقة الجوهرية بين هذه البيانات الرقمية والعملات الافتراضية فتتكرس بالتقائها في العالم الجرمي على الشبكة السوداء.

وفي ظل انهيار القطاع المصرفي في لبنان وامتناع الدولة عن سداد ديونها منذ أوائل ٢٠٢٠، وفقدان الليرة اللبنانية قيمتها بشكل دراماتيكي في ثالث أسوأ انهيار اقتصادي منذ عام ١٨٥٠ بحسب البنك الدولي. ساهم التضخم الحاصل وانهيار العملة اللبنانية وخسارة الليرة أكثر من ٩٥% من قيمتها، وتآكل الرواتب وحجز المصارف لودائع اللبنانيين بالعملات الصعبة، في تفتيش الناس عن الاستثمار في العملات الرقمية للتخلص من فقدان القيمة.

وتعتبر قضية تنظيم العملات المشفرة وتحديد التقنيات الرقمية من القضايا الرئيسية التي تحتاج إلى معالجة متعددة الأطراف. على الرغم من أن العديد من المبادرات قد تم تطويرها في جميع أنحاء العالم لإنشاء مثل هذا التنظيم، ويقتضي فهم تلك الجهود وتعزيز مبادئ حقوق الإنسان في جميع أنحاء الصناعة الرقمية، لان تقنية البلوكتشين عابرة للحدود حيث إنها لا تعرف الحدود الوطنية كعملة أو تقنية وتطلب نهجاً موحداً ومتعدد الأطراف للتنظيم.

وتأثر لبنان بالتحويلات الرقمية وتفاعل معها في كل الاتجاهات وكانت تحضيرات جديّة من مصرف لبنان لإصدار عملة لبنانية رقمية مع نهاية عام ٢٠١٩ وحالت الظروف دون ذلك. وكذلك لم يصدر أي قانون بموضوع العملة المشفرة وتعيينها المنتشر على الأراضي اللبنانية. وكان أصدر حاكم مصرف لبنان بصفته رئيس هيئة الأسواق المالية عام ٢٠١٨ حظراً على المؤسسات المالية المرخصة على إصدار نقود إلكترونية ومنع تسويق العملات الرقمية أو التداول بها، لحسابها أو لحساب عملائها، بصورة مباشرة أو غير مباشرة، بما فيها المتداولة في الأسواق المالية المنظمة. وفي عام ٢٠٢٠ حظر مصرف لبنان إصدار النقود الإلكترونية من أي كان والتعامل بها بأي شكل من الأشكال الا وفقاً لاحكام القرارات الصادرة والتي ستصدر عن مصرف لبنان. علماً أن هناك عدد من القوانين والأنظمة والتعاميم التي رعت الدفع والمعاملات الإلكترونية ومكافحة تبييض الأموال وتمويل الإرهاب وجرائم المعلوماتية كما يوجد مكاتب متخصصة بملاحقة هذه الجرائم.

أظهرت الأبحاث أن حوالي ثلث السكان فقط يمكنهم فهم البيانات والإحصائيات التي تشكل مخرجات حركة البيانات المفتوحة. وتذهب تقنية البلوكتشين إلى أبعد من ذلك بكثير حيث تتطلب من المواطنين قبول

نهج جديد تمامًا لإدارة البيانات وأن يكون لديهم بعض الفهم للتشفير ومبادئ الإدارة الرئيسية أو مواجهة خسارة أموالهم أو خدماتهم الحكومية. إن الانتقال إلى اقتصاد رقمي بالكامل دون تحديث أنظمتنا التعليمية هو وصفة كارثية مؤكدة.

بعد نهوض لبنان من كبوته لا بد من اقامة ورشة تشريعية والتركيز على التعليم وفئة الشباب ودعم المؤسسات الناشئة والاعتماد على الاعتراف اصلاح القوانين الرقمية الحامية لان المطلوب أن يكون العاملون في الخدمة المدنية والجزائية والقضاة والضباط العدليين في مكاتب الملاحقة أكثر من مجرد مُلمين بالتقنية. وعليه نقترح التوصيات التالية والتي تصلح لكل الدول:

١- خلق بيئة الابتكار لاستخدامات قانونية للتقنيات الحديثة ونشر الوعي لاهميته وكيفية حمايته وإدخالها ضمن المنهج الدراسي ومنذ الصفوف الابتدائية، وضرورة إدراك أهمية التعليم للجميع وكيفية إدارة الطرق السريعة للبيانات التي يتم بناء مجتمعنا عليها الآن وفي المستقبل.

٢- اعتماد الهوية الرقمية، وتعزيز الموثوقية وشبكة الحماية لإتاحة المجال أمام الأفراد والشركات الصغيرة والمتوسطة للوصول إلى الخدمات التي يحتاجون إليها وتعزيز تقنيات الذكاء الاصطناعي الذي يُستخدم في التدقيق والرقابة.

٣- اصدار قانون إطار ينظم المنصات وشروط اصدار النقود الإلكترونية والافتراضية المشفرة ومشاعل التعدين ويضع مبادئ حسن نية للتداول بالعملات المشفرة.

٤- انشاء ودعم "الوكالة الوطنية للأمن ونظم المعلومات" وفق الاستراتيجية الوطنية للأمن السيبراني . تشمل الحماية الدوائر الحكومية والتجارة الإلكترونية والشركات والافراد من الهجوم السيبراني، وكل أشكال القرصنة، أو العبث بالمحتوى، والإرهاب والتنظيم والإشراف على إدارة مخاطر هذه التقنيات الحديثة بشكل أكثر فاعلية بهدف توفير بيئة عمل آمنة تسهل التعاون ومشاركة البيانات بالتعاون الوثيق مع مزودي الخدمات المعتمدين والخاضعين للقانون وللرقابة والتدقيق.

٥- وضع قانون جزائي مرن لجرائم الانترنت يكون قانون إطار واعتماد المراسيم والنظم المتحركة، يمكن الإعتماد فيه على الاجتهاد الدولي وللمحاكم أن تستند الى القضية المحكوم بها في الفضاء السيبراني، والتي يمكنها مواكبة ما يستجد.

٦- إنشاء نيابة عامة ومحكمة جزائية متخصصة بالانترنت تتبع الجهاز القضائي ويمكن لكل شخص أو كيان حول العالم التقاضي لديها عبر الانترنت مع احترام القواعد الثابتة في القانون الدولي الخاص، ولها أصول محاكماتها على أن يتم تعزيز الجهة الشرطية التي تتولى الملاحقة والتنسيق دوليا عبر الانترنت.

٧- إنشاء غرفة في المحكمة التجارية افتراضية تتعاطى بالنظر في نزاعات العقود الذكية. إذ لا يمكن ترك تدوين المعايير الاجتماعية في عقود ذكية ليتم التعامل معها فقط من قبل الشركات الناشئة أو من قبل الشباب الطامح للمال لأن الطريقة التي يتم بها تنفيذها لها تأثير على عدد كبير من الناس وبالتالي

تحتاج إلى إدارتها عبر المجتمع. فالعقد المشفر المكتوب في بلد ما بموجب مجموعة معينة من القوانين له تأثير على مواطني بلد آخر.

٨- إقامة غرف قضائية مفتوحة متخصصة بالانترنت ترتبط بوزارات العدل العربية والتربية والتعليم العالي وربطها بصفحات كل الجامعات العربية وتتبادل الآراء والخبرات وتتلقى الشكاوى وتضع الحلول لتعزيز الثقافة القانونية لدى الطلاب للإطلاع على كل الأنظمة الجديدة والجرائم المستجدة وعقوباتها وخطر اعتماد الشبكة السوداء وتعزيز الوعي المالي وأهمية البيانات الشخصية واحترام الخصوصية في فضاء الانترنت.