الإنترنت المظلم والعملات الافتراضية: التحديات الجديدة للقانون الجنائي

د. وليد بن صالح*

الملخص:

يتناول هذا البحث بالدراسة التحديات التي أصبح يشكلها الإنترنت المظلم والعملات الافتراضية بالنسبة للقانون الجنائي، حيث أثار تزايد حجم الجرائم المرتكبة عبر شبكات الإنترنت المظلم، التي لا تخضع للقواعد القانونية ولرقابة الجهات المنظمة والتي يفوق حجمها الإنترنت السطحي بمئات الأضعاف، قلقاً متزايداً لدى الدول والمنظمات التي تسعى للحد من الآثار السلبية للظواهر الإجرامية. كما يعرض هذا البحث للاستخدام الإجرامي المتزايد للعملات الافتراضية الجديدة وفي مقدمتها "بيتكوين" في معاملات الإنترنت المظلم والتي تشمل اقتناء السلاح والمخدرات وغسيل الأموال. ويكتسي هذا البحث أهميته من تزايد حجم هذه الظواهر الإجرامية على شبكة الإنترنت والمعلومات الدولية، واتساع نطاق التطبيقات والبرامج المستخدمة في ذلك، وهو ما استدعى تعزيز الدول لتشريعاتها وإجراءاتها لمواجهة ذلك، كما اقتضى ذلك تعاوناً دولياً. كما يهدف إلى بيان أوجه قصور الآليات التقليدية للقانون الجنائي وعجزها عن مجابهة المخاطر التي يحملها الإنترنت المظلم والعملات الإلكترونية، وإلى تقديم حلول قانونية من شأنها أن تضمن مكافحة فعالة للجرائم الإلكترونية.

وللإحاطة بهذه التحديات التي يواجهها القانون الجنائي، فقد اعتمد البحث على المنهج الوصفي لإبراز التطور الذي شهدته هذه الظواهر المستجدة وكيفية تعاطي الحكومات والتشريعات معها، كما اعتمد المنهج المقارن في بيان تنظيم التشريعات للجرائم في الفضاء الإلكتروني، مع تركيز واضح على المشرعين التونسي والكويتي. وقد انتهى البحث إلى التوصية بتبني وتعزيز وتطوير وسائل تقصي الجرائم ومكافحتها، وذلك في ظل قصور وسائل التحري التقليدية والحاجة إلى فرض الرقابة على منصات تبادل العملات الافتراضية.

كلمات دالة:

الإنترنت العميق، الجرائم الإلكترونية، الإثبات الإلكتروني، العملات المشفرة، شبكة المعلومات.

* أستاذ القانون الجنائي المشارك، كلية الحقوق والعلوم السياسية، جامعة تونس المنار.

المقدمة:

1. يسود الاعتقاد لدى الكثير من الناس أن القيام ببحث عبر محركات من نوع غوغل (Google) يمكنهم من الوصول إلى أغلب المواقع والمعطيات الموجودة على الإنترنت، إلا أن الواقع مغاير لذلك تمامًا إذ يوجد عالم افتراضي شاسع مخفي ولا يمكن الوصول إليه عبر أي محرك بحث. ويقدر عدد مواقع الإنترنت غير المفهرسة، والمعروفة باسم الإنترنت العميق (Web Deep) بأكثر من 400 إلى 500 مرة من عدد المواقع المتواجدة على الشبكة السطحية المتعارف عليها والقابلة للبحث والفهرسة.

وهذا الإنترنت العميق هو المكان الذي يزدهر فيه الجانب المظلم من الإنترنت، حيث إن جزء الإنترنت العميق المعروف باسم الإنترنت المظلم (Darknet) أصبح ملاذاً للمنظمات الإرهابية والجريمة المنظمة وأضحى تهديداً لأمن الدول. وقد جسدت قضية طريق الحرير (Silk road) نموذجاً حياً للمخاطر التي قد تنشأ عن استعمال الإنترنت المظلم وللأضرار الجسيمة التي يمكن أن تنتج عنه، حيث تم تقييم رقم مبيعات هذه السوق الافتراضية التي تباع فيها جميع الممنوعات بأكثر من 1.2 مليار دولار في جويلية/يوليو 2013. كما ارتاد هذه السوق أكثر من 150 ألف متعامل و4 آلاف بائع مجهولي الهوية.

وقد مثَّل اعتقال مؤسس هذه السوق «روس ويليام أولبريشت» المكنى بـ«Dread Pirate Roberts» في أكتوبر 2013 نقطة انطلاق اهتمام الجمهور العريض بالإنترنت المظلم (Darknet)[1]. كما أصبحت العملات الافتراضية اللامركزية والتي لا يمكن تعقبها جذابة بالنسبة للذين يريدون تحويل الأموال عبر الحدود أو الذين يريدون ممارسة نشاطات غير قانونية عبر الإنترنت بصفة مجهولة (anonymous)، ف«البيتكوين» (Bitcoin) أصبح طريقة الدفع المفضلة في أسواق الإنترنت المظلم[2].

2. منذ ظهوره في سبعينات القرن الماضي مثَّل الإنترنت تحدياً بالنسبة لرجال القانون الذين اجتهدوا لإيجاد حلول للتحديات القانونية التي يطرحها ويزيد من تعقيدها تطوره المستمر والمتواصل، إذ إنه وبمرور السنوات برز الإنترنت أكثر فأكثر كمجال

(1) Rudesill, Dakota S. and Caverlee, James and Sui, Daniel, The Deep Web and the Darknet: A Look Inside the Internet's Massive Black Box (October 20, 2015). Woodrow Wilson International Center for Scholars, STIP 03, October 2015; Ohio State Public Law Working Paper No. 314. Available at: SSRN: https://ssrn.com/abstract=2676615 or http://dx.doi.org/10.2139/ssrn.2676615.

(2) Bal) A,(«Bitcoin and Money Laundering»,
http://www.offtax.com/articles/bitcoin-and-money-laundering.php.VgFN-rVtJ-0.twitter

متاح للمجرمين وللمنظمات الإجرامية التي تجعل من تقنيات الاتصال والتواصل وسائل تمكنها من ارتكاب جرائم يصعب كشفها وإثباتها وزجرها. وتسببت هذه التقنيات في ظهور أنواع جديدة من السلوكيات الإجرامية إضافة إلى أنها أصبحت أداة مميزة لارتكاب جرائم كلاسيكية كالنصب والاحتيال والاختلاس وغسيل الأموال. وإذا كانت شبكة الإنترنت مساحة للحرية، فإن هذه الحرية لا يمكن أن تكون مطلقة، فهي لا يجب أن تمس من سلامة وكرامة الأشخاص أو من سلامة المعاملات المالية، وهو ما جعل مجابهة هذا التهديد الإجرامي الجديد الذي لا يأبه بالزمان أو بالمكان أو بالقوانين ضرورة.

3. وقد وعت مختلف الدول بالخطر الذي تمثله الجرائم الإلكترونية مما دفعها إلى سن تشريعات تهدف إلى التصدي لها وتجريمها وعقابها، كما تم تطوير تقنيات من شأنها الكشف عن هذه الجرائم (كالتعرف على عنوان (IP) المجرم وحجز المعدات الإلكترونية...).

وفي تونس سعى المشرع منذ سنة 1999 إلى وضع نصوص لزجر الجرائم الإلكترونية[3]. ففي مرحلة أولى سعى المشرع إلى زجر الجرائم التي تمس الوسائل المعلوماتية، فقام بتنقيح المجلة الجزائية من خلال القانون عدد 89 لسنة 1999 المؤرخ في 2 أوت/أغسطس 1999 الذي يتعلّق بتنقيح وإتمام بعض أحكام المجلة الجزائية وأضاف الفصلين 199 مكررا[4] و199 ثالثاً ونقح الفصل 172 من نفس المجلة[5]. وقد

(3) يمكن تعريف الجريمة الإلكترونية بكونها: «كل تصرف مخالف للقانون يقع باستعمال عمليات إلكترونية ويهدف إلى المساس بسلامة النظم المعلوماتية والبيانات المعالجة من قبلها».
انظر: Ec 2007, Cybercriminalité: défi mondial et réponses, Quémener et Ferry, –nomica..

(4) ينص الفصل 199 مكرراً (أضيف بالقانون عدد 89 لسنة 1999 المؤرخ في 2 أوت 1999) على أنه: "يعاقب بالسجن من شهرين إلى عام وبخطية (غرامة) قدرها ألف دينار أو بإحدى هاتين العقوبتين فقط، كل من ينفذ أو يبقى بصفة غير شرعية بكامل أو بجزء من نظام البرمجيات والبيانات المعلوماتية. وترفع العقوبة إلى عامين سجناً والخطية إلى ألفي دينار إذا نتج عن ذلك ولو عن غير قصد إفساد أو تدمير البيانات الموجودة بالنظام المذكور. ويعاقب بالسجن مدة ثلاثة أعوام وبخطية قدرها ثلاثة آلاف دينار كل من يتعمد إفساد أو تدمير سير نظام معالجة معلوماتية. ويعاقب بالسجن مدة خمسة أعوام وبخطية قدرها خمسة آلاف دينار كل من يدخل بصفة غير شرعية بيانات بنظام معالجة معلوماتية من شأنها إفساد البيانات التي يحتوي عليها البرنامج أو طريقة تحليلها أو تحويلها، وتضاعف العقوبة إذا ارتكبت الفعلة المذكورة من طرف شخص بمناسبة مباشرته لنشاطه المهني، والمحاولة موجبة للعقاب".

(5) ينص الفصل 199 ثالثاً (أضيف بالقانون عدد 89 لسنة 1999 المؤرخ في 2 أوت 1999) على أنه: «يعاقب بالسجن مدة عامين وبخطية قدرها ألفا دينار كل من يدخل تغييراً بأي شكل كان على محتوى وثائق معلوماتية أو إلكترونية أصلها صحيح شريطة حصول ضَرر للغير، ويعاقب بنفس العقوبات كل من يمسك أو يستعمل عن قصد الوثائق المذكورة، ويضاعف العقاب إذا ارتكبت الأفعال المذكورة من موظف عمومي أو شبهه، والمحاولة موجبة للعقاب.»

واصل المشرع التونسي هذا النهج من خلال سن قوانين زاجرة للجرائم المرتكبة عبر الوسائل الحديثة من خلال القانون عدد 83 لسنة 2000 مؤرخ في 9 أوت/ أغسطس 2000 الذي يتعلق بالمبادلات والتجارة الإلكترونية، والقانون عدد 1 لسنة 2001 مؤرخ في 15 جانفي/يناير 2001 القاضي بإصدار مجلة الاتصالات، وقد سن المشرع فيما بعد ذلك عدداً من القوانين المجرمة كان آخرها القانون الأساسي عدد 26 لسنة 2015 مؤرخ في 7 أوت/أغسطس 2015 الذي ينظم مكافحة الإرهاب ومنع غسيل الأموال.

كما وعى المشرع الكويتي لأهمية مكافحة الجرائم المعلوماتية، وبقصور النصوص الجزائية التقليدية عن مواجهة هذه الجرائم المستحدثة "التي تعتمد في ارتكابها على وسائل التقنية المتطورة، وحماية لحريات الأشخاص وشرفهم وسمعتهم، ودرءًا للعدوان على الأموال والممتلكات العامة والخاصة"[6]، قام بسن القانون رقم 63 لسنة 2015 في شأن مكافحة جرائم تقنية المعلومات.

وقد تبنت معظم الدول العربية قوانين تهدف إلى مكافحة الجرائم الإلكترونية على غرار دولة الإمارات (مرسوم بقانون 5 لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات) ودولة قطر (قانون رقم (14) لسنة 2014 بإصدار قانون مكافحة الجرائم الإلكترونية).

وعموماً فقد تمكن رجال القانون في مختلف الدول على مر السنوات من رفع التحدي القانوني. وقد استقر مشرعو القوانين على عدم اللهاث وراء التطورات التكنولوجية بل اختاروا الاعتماد على قواعد عامة تنطبق عليها[7].

4. لكن بظهور الإنترنت المظلم (Darknet) والعملات الإلكترونية المشفرة (Crypto–currency) أصبح بالإمكان تحويل الأموال عبر الحدود وممارسة نشاطات غير قانونية عبر الإنترنت بصفة مجهولة (Anonymous) باستعمال شبكة «تور» (TOR) كما أن «البيتكوين» (Bitcoin) تلك العملة التي لم يصدرها أي بنك مركزي والتي لا يمكن تعقبها أصبحت طريقة الدفع المفضلة في الأسواق الافتراضية للتجارة غير الشرعية، وهي الأسواق التي تزدهر فيها تجارة الأسلحة والمخدرات وعمليات غسيل الأموال، وهو ما جعل من الآليات التي تم تطويرها لمكافحة الجرائم الإلكترونية بالية، فرواد الإنترنت المظلم يقومون بتشفير عناوين النفاذ إلى

(6) المذكرة الإيضاحية للقانون رقم 63 لسنة 2015 في شأن مكافحة جرائم تقنية المعلومات.

(7) Charpenel (Y), «Le Darkweb, un objet juridique parfaitement identifié Le paradis, lènfer ؟», Dalloz, IP/IT 2017, p.71.

الإنترنت (IP) مما يجعل تحديد أماكنهم مستحيلا، ولا يستعملون وسائل الدفع البنكية التقليدية مما يجعل تعقب معاملاتهم المالية غير ممكن.

5. يمكن تعريف الإنترنت المظلم بكونه مجموعة من الشبكات الخاصة التي يستوجب الدخول إليها استعمال الأدوات اللازمة التي تمكن من إخفاء الهوية، إذ إن الإبحار لا يمكن أن يتم إلا بصفة مجهولة (Anonymous) [8]. والإنترنت المظلم هو جزء من الإنترنت العميق[9] الذي يجمع المعطيات غير المفهرسة من قبل محركات البحث والتي يجب استعمال برنامج خاص أو ترخيص خاص للنفاذ إليها. أما الميزة الأساسية لهذا النوع من الإنترنت فهي إمكانية التخفي شبه المطلق التي يمنحها لمستخدميه[10].

6. أما العملات[11] الافتراضية فهي عملات إلكترونية لا توجد إلا على الإنترنت، وهي ليست صادرة عن أي دولة أو حكومة أو بنك مركزي، وتعمل هذه العملات التي يعتبر أشهرها "البيتكوين" عبر شبكات نظير إلى نظير (P2P– Peer to Peer) ويتم إنشاء هذا النوع من الشبكات (P2P) عند تشغيل العديد من الأفراد للبرامج الضرورية على أجهزة الحاسوب الفردية الخاصة بهم والاتصال ببعضهم البعض؛ لا تملك شبكات P2P موقعًا مركزيًا أو خادماً (سيرفر Server) أو تنظيماً، ف"البيتكوين" ليس له فريق تسيير ولا وجود مادي في أي مكان[12].

وتطرح مسألة الطبيعة القانونية للعملات الافتراضية جدلاً، فهل يتعين اعتبارها عملة أو وسيلة دفع أو مالاً؟[13]، وقد اعتبر مجلس الدولة الفرنسي في قراره عدد (417809) الصادر في 2018/04/28 أن وحدات "البيتكوين" تمثل مالاً منقولاً معنوياً (incorporels meubles Biens)[14].

(8) De Maison Rouge (O.), Darkweb: plongée en eaux troubles, Dalloz, IP/IT, 2017 p.74.

(9) يمثل الإنترنت العميق (Deep Web) ما نسبته 95% من الإنترنت، في حين يمثل الإنترنت (Clear web) الذي يشمل المعطيات المفهرسة من قبل محركات البحث (Bing Yahoo, Google, ...) 5% من الإنترنت.

(10) Petit (A), Visite guidée du Darkweb cybercriminel, Dalloz IP/IT, 2017, p.86.

(11)بالنسبة للجدل حول هل يمكن اعتبارها عملة أم لا، انظر:

Marain (G), Le bitcoin à l'épreuve de la monnaie, AJ contrat 2017, p.522.

(12) Christopher, Catherine Martin, Whack–a–Mole: Why Prosecuting Digital Currency Exchanges Won't Stop Online Laundering 2014, 18 Lewis & Clark L. Rev. 1 (2014). Available at SSRN: https://ssrn.com/abstract=2312787.

(13) Pierre Storrer, Crowdfunding, bitcoin : quelle régulation? , D. 2014, P.832.

(14) Conseil d'État – 26 avril 2018 – n° 417809.

7. وقد عرفت السنوات الأخيرة الماضية تضاعف الجرائم المتعلقة بالإنترنت المظلم والعملات الافتراضية مما دفع سلطات عدة دول (كدول الاتحاد الأوروبي وكوريا الجنوبية ...) إلى التعبير عن إرادتها في سن قوانين من شأنها الحد من إمكانية الإبحار بصفة مجهولة والتشفير، إضافة إلى تنظيم وتعديل العملات الإلكترونية. فإذا كانت شبكة الإنترنت مساحة للحرية، فإن هذه الحرية لا يمكن أن تكون مطلقة، إذ لا يجب لها أن تمس من حقوق وكرامة الأشخاص أو من سلامة المعاملات المالية.

وفي ضوء ذلك، يجدر التساؤل حول التحديات التي تطرحها هذه التكنولوجيات المستحدثة والتدابير الواجب اتخاذها للحد من خطرها الإجرامي؟

إن ظهور الإنترنت العميق بشكل عام والإنترنت المظلم بشكل خاص، إضافة إلى التطور الكبير للعملات الافتراضية يمثل تحدياً جديداً لرجال القانون (سواء أكانوا مكلفين بصياغة القانون أم بإنفاذه) (المطلب الأول)، فهذا الفضاء يمثل نظامًا اقتصادياً واجتماعيًا وسياسيًا جديدًا مصممًا للوجود والعمل بعيدًا عن متناول القانون والرقابة الحكومية[15]. وبالتالي فإن زجر الجرائم المرتكبة في هذا الفضاء يستوجب فهماً عميقاً لآليات عمله وتفرض تبني إجراءات مستحدثة (المطلب الثاني).

(15) Rudesill, Dakota S. and Caverlee, James and Sui, Daniel, The Deep Web and the Darknet: A Look Inside the Internetos Massive Black Box (October 20, 2015). Woodrow Wilson International Center for Scholars, STIP 03, October 2015؛ Ohio State Public Law Working Paper No. 314. Available at SSRN: https://ssrn.com/abstract=2676615 or http://dx.doi.org/10.2139/ssrn.2676615

المطلب الأول

قصور الآليات التقليدية للقانون الجنائي

بالرغم من تبني المشرع في تونس والكويت لنصوص قانونية تهدف إلى زجر الجرائم الإلكترونية، فإن هذه النصوص تبقى منقوصة وغير متلائمة مع تطور الإنترنت المظلم (الفرع الأول) وبروز العملات الافتراضية (الفرع الثاني).

الفرع الأول

تحدي زجر الجرائم على الإنترنت المظلم

8. إن الإنترنت المظلم هو شبكة معلومات عالمية خاصة تمكن المستخدمين من إجراء معاملات مجهولة دون الكشف عن أي أثر لمواقعهم. وتعتبر شبكة "تورTOR " واحدة من أهم هذه الشبكات الخاصة، وتستعمل أجهزة الحاسوب على هذه الشبكة بروتوكول اتصالات مشفرة لا يمكن الولوج إليها عبر متصفحي الإنترنت العاديين[16]. ويستوجب الدخول إلى هذ الشبكة استعمال برنامج خاص على غرار برنامج «تور» (TOR)[17] الذي يعتبر أشهر هذه البرامج وبوابة الدخول للإنترنت المظلم. ويُمكّن هذا البرنامج من الإبحار بصفة مجهولة تمنع نظرياً إمكانية تحديد مكان أو هوية المبحر، أي أنه نظرياً لا يمكن تحديد عنوان المستخدم(IP)[18].

9. وتُمكِّن شبكة "تور TOR" من حماية اتصالات المستخدم من نوعين من الرقابة: أولاً: تمكن هذه الشبكة من الإبحار على صفحات الويب العادية (World Wide Web) بإظهار عنوان آخر غير العنوان الحقيقي للمستخدم، وبالتالي فإن شخصاً متواجد في نيويورك يقوم بإخفاء هويته عبر مجموعة من الخوادم الوسيطة «بروكسي proxies»، يكون آخرها في القاهرة، وسيظهر بالنسبة للصفحة وكأنه متواجد بالقاهرة. ثانياً: يمكن للأشخاص استخدام شبكة «تور TOR» لحماية اتصالاتهم من خلال ميزة الخدمات الخفية لهذه الشبكة، والتي تسمح لمن يريد باستضافة المحتوى أو الخدمات دون كشف الموقع الفعلي لخوادمه. هذه الخدمات المخفية يمكن الوصول إليها فقط من قبل أولئك الذين يستخدمون البرمجيات التي تمكنهم من ولوج شبكة «تور TOR». وحتى الاتصالات بين خدمة خفية (الأسواق غير الشرعية من نوع (AlphaBay وRoad Silk) ومستخدميها تحدث عبر"نقطة

(16) من نوع مايكروسوفت إيدج «Edge Microsoft» أو غوغل كروم «Google Chrome».

(17) مختصر لـ«The Onion Router» كما توجد برامج أخرى تسمح بالدخول للإنترنت المظلم مثل GNU, freenet, I2P, Zeronet, SafetyGate...

(18)في الواقع التخفي المطلق على الإنترنت غير ممكن، إلا أن استعمال هذا النوع من البرامج يجعل التعرف على هوية المبحر على الإنترنت المظلم صعباً جداً، وهو ما يفسر تواجد أجهزة الشرطة والاستخبارات بهذا الفضاء (على غرار الـNSA و FBI الأمريكيتين و FSB الروسية و الأوروبية Europol....).

الالتقاء"، وهي عبارة عن بروكسي "Proxy» يوفر طبقة إضافية من الحماية.

ويدعي بعض مناصري الحريات المدنية أن استعمال برمجيات إخفاء الهوية من شأنه حماية حرية التعبير والحياة الشخصية، كما قد ترغب الشركات التجارية في استخدام شبكة (تور TOR) لمنع الجواسيس المختصين في الشؤون الاقتصادية من الحصول على أي ميزة تنافسية عن طريق التعرف على نشاطات موظفيهم ومع من يتواصلون أو ما هي الموضوعات التي يبحثون عنها. بالإضافة إلى ذلك تمكن هذه الشبكة من الالتفاف على تقنيات الحجب التي يتم استعمالها من قبل الدول لمنع الولوج إلى بعض المواقع الممنوعة[19].

10. لئن كان رواد ومناصرو الإنترنت المظلم يدعون أن له فوائد عديدة تتمثل في توفير مساحة للحرية بعيداً عن الرقابة، فإن هذا الفضاء أصبح في الواقع ملاذاً للعمليات غير الشرعية لمستخدمي الإنترنت الراغبين في التخفي[20]. فبالنظر لميزات الإنترنت المظلم تدفق المجرمون على هذا الفضاء للتمتع بمنظومة مأمونة تضمن إخفاء الهوية وتتيح التحادث والتنسيق والفعل. ويستعمل المجرمون الحديثون هذا الفضاء لارتكاب جرائم تعتمد على التكنولوجيا، مثل قرصنة الكمبيوتر، سرقة الهوية، التحيل ببطاقة الائتمان، وانتهاك حقوق الملكية الفكرية إذ يُعَدُّ الإنترنت المظلم مجالاً متاحاً لتبادل الأفلام والموسيقى وبيع المنتوجات المقلدة.

كما يستعمل المجرمون التقليديون والمنظمات الإجرامية التقليدية الإنترنت المظلم لعولمة عملياتهم مع التمتع بإمكانية الإفلات من العقاب ولتسهيل ارتكاب جرائم تجري تقليديًا في العالم الفعلي، مثل تزييف العملة، ترويج المخدرات، استغلال الأطفال[21]، الاتجار بالبشر، الاتجار بالأسلحة والذخيرة، القتل[22]، والإرهاب[23].

(19) Ghappour (A), Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web, Stanford Law Review, Vol. 69, Issue 4, April 2017: UC Hastings Research Paper No. 170.
Available at: https://www.stanfordlawreview.org/print/volume-69/issue-4/.

(20) De Maison Rouge (O), Darkweb: plongée en eaux troubles, Dalloz IP/IT 2017, p.74.

(21) Goodman (M), Future crimes: everything is connected, everyone is vulnerable, and what we can do about it" 194 (2015): Press Release, U.S. Att'y's Office for the S. Dist. of N.Y., U.S. Dep't of Justice, Ross Ulbricht, A/K/A "Dread Pirate Roberts," Sentenced in Manhattan Federal Court to Life in Prison (May 29, 2015), https://www.justice.gov/usao-sdny/pr/ross-ulbricht-aka-dread-pirate-roberts-sentenced-manhattan-federal-court-life-prison.

(22) Greenberg (A), Meet the 'Assassination Market' Creator Who's Crowdfunding Murder with Bitcoins, FORBES (Nov. 18, 2013, 8:30 AM), http://www.forbes.com/sites/andygreenberg/2013/11/18/meet-the-assassination-market-cr-ator-whos-crowdfunding-murder-with-bitcoins/2277df031ac1.

(23)حسب السلطات الألمانية تمكن علي دافيد سنبلي على الأغلب من شراء السلاح الذي مكنه من قتل تسعة =

كما أن عدة مجموعات إجرامية منها مجموعات إرهابية تقوم بتمويل نشاطاتها عبر الإنترنت المظلم[24].

11. إن استعمال الإنترنت المظلم من قبل المجرمين للتخفي وجعل اتصالاتهم مجهولة يجعلان تتبع المجرمين مستحيلاً بالنسبة للسلطات المكلفة بإنفاذ القانون. ففي حالات الجرائم المعلوماتية، يعتبر تحديد موقع الكمبيوتر المستخدم من قبل مرتكب الجريمة هو الخطوة الأكثر أهمية في اكتشاف هوية مرتكب الجريمة وفي جمع الأدلة اللازمة لإدانة المشتبه به. وبدون التوصل إلى جهاز كمبيوتر الجاني، سيفتقر المحققون والنيابة العمومية للأدلة التي تمكنهم من نسب السلوك الإجرامي الافتراضي لشخص حقيقي. فالتقنيات التقليدية للبحث تعتمد على تجميع المعطيات من قبل طرف ثالث، إذ تنطلق الأبحاث عامة في الجرائم الإلكترونية من معلومات غير موصوفة حول مرتكب الجريمة على غرار عنوان البريد الإلكتروني الذي استعمله، وعلى إثر ذلك يمكن للمحققين طلب معلومات حول الحساب المقترن مع هذا البريد من قبل الطرف الثالث ألا وهو مزود عنوان البريد الإلكتروني (e-mail provider)[25]. وقبل ظهور الإنترنت المظلم كانت هذه المعلومات تمكن من الحصول على معلومات تساعد على كشف هوية مرتكب الجريمة على غرار عنوان الولوج إلى الإنترنت (IP Internet Protocol) . وقد يحتفظ مزود خدمة الإنترنت بسجلات شاملة، وفي هذه الحالة تسمح المحاكم الأمريكية بأن تشمل المعلومات التي يفصح عنها مزود خدمات الإنترنت معلومات إضافية مثل عنوان إرسال الفواتير ورقم الهاتف[26]. وانطلاقاً من هذه المعلومة يمكن التوصل إلى مكان تسجيل دخول المستخدم ومصادرة الجهاز مادياً بعد الحصول على إذن قضائي واستخراج المعطيات الموجودة به[27].

بالطبع يحدث في العديد من المرات أن يتواجد مرتكب الجريمة خارج الدولة التي وقعت بها الجريمة، وفي هذه الحالة يتعين اللجوء إلى طرق التعاون الدولي لتحصيل الأدلة، وخاصة منها اتفاقيات التعاون القضائي الدولية والإقليمية والثنائية.

= أشخاص والانتحار بميونيخ في 22/7/2016 من خلال الإنترنت المظلم. انظر:
Ruth Bender & Christopher Alessi, Munich Shooter Likely Bought Reactivated Pistol on Dark Net, WALL ST. J. (July 24, 2016, 4:23 PM ET), http://www.wsj.com/articles/munich-shooter-bought-recommissioned-pistol-on-dark-net-1469366686; Ghappour (A), Op. cit.

(24) De Maison Rouge (O), Op.cit., p.74.

(25) تتعقد العملية إذا كان المزود متواجداً خارج الدولة التي تجري بها التحقيقات، إذ يجب اتباع بروتوكولات ديبلوماسية حتى تعطي الدولة التي يوجد بها المزود المعلومات.

(26) United States v. Kennedy, 81 F. Supp. 2d 1103, 1107 (D. Kan 2000).

(27) Ghappour (A), Op. cit.

12. لكن لجوء الجاني إلى الإنترنت المظلم يجعل هذه الطرق التقليدية في جمع الأدلة بالية، إذ إنه في هذه الحالة يبدو وكأن هذا الأخير قد قام بتسجيل دخوله انطلاقاً من واحد من بين آلاف الكمبيوترات البروكسي «Proxy» بدلاً من الكمبيوتر الذي يستعمله. وبالتالي من دون إمكانية التوصل إلى المكان الحقيقي للكمبيوتر المستخدم لا يمكن للمحققين استعمال طرق التحقيق التقليدية لإثبات توفر أركان الجريمة[28].

بالإضافة إلى ذلك، فإن مطاردة الجاني على الإنترنت المظلم تفرض قيودًا أخرى، فالجاني الذي يستعمل الإنترنت المظلم يتمكن من إخفاء هويته لتسجيل الدخول لمزود البريد الإلكتروني مثلاً، مما يجعل طرق التحري التي تعتمد على طرف ثالث يتولى توفير المعطيات غير ذي جدوى، وبالتالي لا يوجد أو يوجد عدد قليل من المشغلين التقنيين الذين يمكن الاعتماد عليهم لتحديد مكان الجاني وجمع الأدلة والإثباتات.

كما أن مستخدمي الإنترنت المظلم هم أشخاص حذرون لا يقومون عادة بتحميل معطيات غير قانونية ولا يقومون بالدفع باستخدام وسائل الدفع الكلاسيكية مفضلين استعمال "البيتكوين"، وهو ما يجعل آليات الاعتراض وحجز الأجهزة والمعطيات غير ناجعة، كما أن إمكانية إخفاء الهوية تمنع أي زجر للجرائم المرتكبة[29]. إن اللجوء للإنترنت المظلم يمكن المجرمين والمنظمات الإجرامية من ممارسة نشاط إجرامي سري لا يمكن تعقبه وذلك على نطاق واسع، كما أن سهولة استعمال برمجيات إخفاء الهوية وصعوبة الكشف عن هذه الجرائم تبرزان التحدي الذي تواجهه السلطات، خاصة وأن عملة الدفع في هذا الفضاء تتمثل في العملات الافتراضية.

الفرع الثاني
تحدي استعمال العملات الافتراضية

13. بغرض إخفاء الهوية يعمد مستخدمو الإنترنت المظلم إلى استعمال العملات الافتراضية على غرار "البيتكوين"(Bitcoin) الذي يعتبر أول عملة افتراضية مشفرة في العالم (Cryptocurrency). وانتقلت هذه العملة من ظاهرة اقتصادية هامشية إلى ظاهرة عالمية في أواخر عام 2017 بالنظر إلى السعر الصاروخي الذي أصبحت تتداول به[30]. وقد تم اقتراح فكرة "البيتكوين" سنة 2008 في شكل ورقة بيضاء من قبل مطور برمجيات اسمه المستعار ساتوشي ناكوموتو، وكان محاولة لتفعيل النقود الإلكترونية كبديل عن الخدمات المصرفية التقليدية في أعقاب الأزمة

(28) Ghappour (A), Op. cit.
(29) Saenko (L), Op. cit.
(30) Peter Rudegeair and Akane Otani, Bitcoin Mania: Even Grandma Wants In on the Action, The Wall Street Journal, November 29, 2017. (https://www.wsj.com/articles/bitcoin-mania-even-grandma-wants-in-on-the-action-1511996653).

المالية العالمية. عند صدوره في 2009 كانت قيمة "البيتكوين" الواحد أقل من سنت واحد في الولايات المتحدة الأمريكية، لتبلغ قيمته بعد تسع سنوات فقط[31]، نحو 16 ألف دولار في جانفي/يناير 2018 [32]، كما بلغت قيمة سوق العملات الإلكترونية المشفرة أكثر من 200 مليار دولار[33].

14. ولئن كان استعمال هذه العملات لا ينحصر في إطار الإنترنت المظلم، فإن تداولها يتم بصفة مجهولة، إذ إن المعاملات ب"البيتكوين" تظهر في شكل حسابات لا تحمل هوية صاحبها، وهو ما يجعلها رائجة الاستعمال لدى المهربين والمجرمين وعمليات دفع المعاملات المشبوهة. إن مستعملي "البيتكوين" يستخدمون أسماء مستعارة بدلاً من أسمائهم الحقيقية، كما أن هذه العملة يمكن تحويلها دون وسطاء عبر حدود الدول بسهولة تامة تضاهي سهولة إرسال بريد إلكتروني، وتتميز هذه العملة باستقلالها التام وعدم تنظيمها، كما أنها غير مقيدة بدولة أو بنك مركزي، ويقوم النظام على علاقة ثقة من خلال تشكيل شبكة peer to peer لتسهيل تبادل المعطيات بين المستخدمين، كما أن تخزين "البيتكوين" لا يتم في سيرفر واحد مركزي. وقد كشفت دراسة أن أسواق الإنترنت المظلم كـ"road Silk " ومن بعدها "AlphaBay" مصدر تقريباً كل "البيتكوين" الذي تم غسيله عبر منصات تداول العملات الإلكترونية[34].

15. ويتعزز خطر تبييض الأموال باستعمال بطاقات دفع بعملات حقيقية ملتصقة بحسابات بيتكوين (Bitcoin to plastic or BTC2 Plastic Card). وقد ظهرت هذه البطاقات سنة 2013 وهي بصدد التطور بسرعة، فالرصيد المتوفر على هذه البطاقة بالعملة الحقيقية يعادل قيمة "البيتكوين" المملوكة، وتمكن هذه البطاقات من الدفع بالعملة الحقيقية لدى تاجر حقيقي أو إلكتروني، كما تمكن من سحب نقود من موزعي الأموال الآلية التي تنتمي إلى شبكات عالمية معروفة من نوع "Visa" و"Mastercard". وتستعمل هذه الإمكانية المتاحة المسماة "cash out" من قبل المجرمين لسحب أموال الأرباح المكتسبة ب"البيتكوين" نقداً، وتكون هذه الأرباح عادة ناجمة عن بيع سلع ممنوعة على الإنترنت المظلم (مخدرات، أسلحة،

(31)تمكن بعض الأشخاص من تحقيق أرباح هائلة بفضل الارتفاع الصاروخي لسعر "البيتكوين" والعملات الإلكترونية، انظر:

Samuel Gibbs ,Man buys 27$ of bitcoin ,forgets about them ,finds they're now worth 886$k ,The Guardian) UK ,(December) .2015 ,8 https//:www.theguardian.com/technology/2015/dec/09/bitcoin-forgotten-currency-norway-oslo-home)

(32)عرفت سنة 2018 انهيار قيمة "البيتكوين" لتبلغ في تاريخ كتابة هذه الأسطر 6822 دولار أمريكي،

(33) Yaya J. Fanusie and Tom Robinson, Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services, January 12, 2018, https://info.elliptic.co/whitepaper-fdd-bitcoin-laundering.

(34) Yaya J. Fanusie and Tom Robinson, Op. Cit.

وثائق هوية مزيفة، هويات بنكية مسروقة...)[35]. كما أكد الجهاز الأمريكي المكلف بمكافحة المخدرات (DEA–Administration Enforcement Drug) أن "البيتكوين" يقع استعماله لغسيل الأموال تحت غطاء معاملات تجارية (Trade–based money laundering "TBML")[36].

16. وبالرغم من أن هذه العملات الافتراضية تمثل فرصة كبيرة للابتكار المالي، فإن جلبها لانتباه مختلف الجماعات الإجرامية يجعلها تشكل خطرًا إجرامياً مهماً خاصة في مجال تمويل الإرهاب، حيث تسمح هذه التقنية بتحويل الأموال بشكل مجهول دوليًا. ففي حين أن عملية الشراء الأصلي للعملة الافتراضية قد تكون مرئيّة (على سبيل المثال، من خلال النظام البنكي)، فإنه يصعب فيما بعد الكشف عن جميع عمليات التحويل التالية للعملة الافتراضية. وقد لاحظت أجهزة الاستخبارات الأمريكية أن المجرمين يبحثون عن شراء عملات افتراضية تتميز بالصفات التالية: إخفاء هوية المستخدمين والمعاملات؛ القدرة على نقل العائدات غير المشروعة من بلد إلى آخر بسرعة غير عرضة لتقلبات السوق اعتماد واسع النطاق في الجريمة السرية؛ والموثوقية. كما تشعر وكالات إنفاذ القانون بالقلق إزاء استخدام العملات الافتراضية من قبل المنظمات الإرهابية، حيث تم رصد استخدام مواقع إلكترونية تابعة لمنظمات إرهابية للترويج لجمع التبرعات باستعمال "البيتكوين"[37]. بالإضافة إلى ذلك، رصدت هذه الأجهزة مناقشات إلكترونية بين متطرفين تتحدث عن استخدام عملات افتراضية لشراء الأسلحة وتعليم المتطرفين الأقل تقنيًا كيفية استخدام العملات الافتراضية[38].

يتضح بالتالي بصفة جلية الخطر الإجرامي الذي تشكله التوليفة بين الإنترنت المظلم والعملات الإلكترونية المشفرة، وهو ما يجعل تدخل القانون ضرورياً للحد من التجاوزات.

(35) على سبيل المثال قامت السلطات الفرنسية في 17 فبراير 2016 بإلقاء القبض على مجرم إلكتروني فرنسي يعرض للبيع على الإنترنت المظلم أرقام بطاقات مصرفية مسروقة، مقابل الدفع ب"البيتكوين". تم تحويل إيرادات المبيعات إلى محفظة بيتكوين مرفقة ببطاقة BTC2plastic صادرة في الخارج. تم سحب هذه الأموال في وقت لاحق نقداً في موزع نقود آلي، أو أنفقت لشراء أجهزة كمبيوتر عبر الإنترنت. انظر:
Tracfin, Tendances et analyse des risques de blanchiment de capitaux et de financement du terrorisme en 2016, https://www.economie.gouv.fr/files/rapport–analyse–tracfin–2016.pdf.

(36) Drug Enforcement Administration, 2017 National Drug Threat Assessment, https://www.dea.gov/docs/DIR–040–17__2017–NDTA.pdf.

(37) تضمن تقرير فريق العمل المعني بالعمليات المالية الخاصّة بمكافحة تبييض الأموال (FATF) مقالاً عنوانه: «"البيتكوين" وصدقة الجهاد» يشرح كيفية استعمال "البيتكوين" وكيف يمكن توظيفه لتمويل الجهاد. وقد تضمن المقال تفسيراً لكيفية القيام بتبرعات بصفة مجهولة لإرسال الأموال باستعمال "البيتكوين" للمجاهدين.

(38) Financial Action Task Force (FATF) (2015), Op. Cit , pp. 36–37.

المطلب الثاني
ضرورة اعتماد آليات جديدة

17. إن مجابهة التهديد الإجرامي المعلوماتي الجديد الذي لا يأبه بالزمان أو بالمكان أو بالقوانين ضرورة، إذ إنه وفي انتظار تطبيق قواعد صارمة، لا يزال المجرمون يضربون دون عقاب، كما أن معاملاتهم المالية التي كانت تعتمد دائماً على "البيتكوين" في الماضي تنوعت وبدأت في التحول الآن إلى بدائل رقمية أخرى. وهو ما يجعلنا نتساءل عن التدابير الواجب اتخاذها قصد التصدي لهذا الخطر الإجرامي الجديد والذي يطرح تحديات غير مسبوقة للقانون الجنائي. وتفرض مكافحة الجرائم الإلكترونية ملاحقة المجرمين حتى لو تواجدوا على الإنترنت المظلم، إذ لا يجب أن يتحول هذا الفضاء الشاسع إلى منطقة خارجة عن القانون. وقد تم وضع إجراءات تمكن من الكشف على جرائم الإنترنت المظلم والحد من الإجرام الذي يترعرع فيه (الفرع الأول)، كما أن الحد من الجرائم يمر أيضاً عبر مراقبة تداول العملات الافتراضية (الفرع الثاني).

الفرع الأول
اعتماد آليات مناسبة للإنترنت المظلم

18. سواء ارتكبت الجريمة المعلوماتية على الإنترنت العادي (Clearnet) أو الإنترنت المظلم (Darkweb) فهي تندرج تحت القوانين الجنائية نفسها. وبالمثل، فإن قواعد الاختصاص القضائي والقانون المنطبق لا تختلف في الوضوح أو الظلام[39]. فالقانون لا يفرق بين الإنترنت العمومي المتعارف عليه والشبكات الخاصة سواء أكانت مخفية أم لا. إن هذه الشبكات الخاصة حتى وإن لم تكن مفهرسة من قبل محركات البحث من نوع غوغل فهي تبقى قانونياً شبكات تعتمد على نظام معالجة معلوماتية[40]. وبالتالي تعد كل جرائم المعلوماتية المتعارف عليها قائمة بقطع النظر عن الفضاء الذي ارتكبت به، كما أن الجرائم التقليدية كبيع المخدرات والسلاح والنقود

(39) Charpenel (Y), Op. Cit.

(40) في الكويت يُعرِّف القانون رقم 63 لسنة 2015 في شأن مكافحة جرائم تقنية المعلومات نظام المعالجة الإلكترونية للبيانات بأنه: «نظام إلكتروني لإنشاء أو إدخال أو استرجاع أو إرسال أو استلام أو استخراج أو تخزين أو عرض أو معالجة المعلومات أو الرسائل إلكترونياً». كما يُعرِّف الشبكة المعلوماتية بأنها: «ارتباط بين أكثر من منظومة اتصالات لتقنية المعلومات للحصول على المعلومات وتبادلها». كما يُجرم القانون التونسي (فصول 199 مكرر و199 ثالثاً من المجلة الجزائية) جرائم النفاذ أو البقاء غير الشرعي في نظام معالجة آلية للمعلومات والاعتداء على سلامة النظم والبيانات المعلوماتية والتدليس الإلكتروني.

المزيفة تبقى مجرمة سواء ارتكبت باستعمال الإنترنت أو بغيره من الوسائل[41].

19. ويجرم المشرع الكويتي في القانون رقم 63 لسنة 2015 بشأن مكافحة جرائم تقنية المعلومات، كل من أنشأ موقعاً أو نشر معلومات باستخدام الشبكة المعلوماتية أو بأي وسيلة من وسائل تقنية المعلومات بقصد الاتجار بالبشر أو تسهيل التعامل فيهم، أو ترويج المخدرات أو المؤثرات العقلية وما في حكمها، أو تسهيل ذلك في غير الأحوال المصرح بها قانوناً[42]. كما نصت المادة (10) من نفس القانون على أنه: "يعاقب بالحبس مدة لا تجاوز عشر سنوات وبغرامة لا تقل عن عشرين ألف دينار ولا تجاوز خمسين ألف دينار أو بإحدى هاتين العقوبتين، كل من أنشأ موقعاً لمنظمة إرهابية أو لشخص إرهابي أو نشر عن أيهما معلومات على الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات ولو تحت مسميات تمويهية، لتسهيل الاتصالات بأحد قياداتها أو أعضائها، أو ترويج أفكارها، أو تمويلها، أو نشر كيفية تصنيع الأجهزة الحارقة، أو المتفجرة، أو أية أدوات تستخدم في الأعمال الإرهابية".

ويتبين من صياغة هذه النصوص أنها تشمل الإنترنت المظلم الذي يُعد شبكة معلوماتية وتقنية معلومات، وبالتالي فجرائم الاتجار بالبشر وترويج المخدرات والجرائم الإرهابية وغيرها من الجرائم التي نص عليها القانون رقم 63 لسنة 2015 تبقى قائمة حتى لو تم ارتكابها باستخدام الإنترنت المظلم.

20. إلا أن تجريم الأفعال وحده لا يعني زجراً فعالاً للجرائم التي ترتكب على الإنترنت المظلم، إذ إن هذا الإنترنت يطرح إشكالية وسائل التقصي التي يتعين اعتمادها للكشف عن هذه الجرائم في ظل قصور وسائل التحري التقليدية، حيث إنه يصعب الكشف عن الجاني إذا استعمل برامج إخفاء الهوية.

وتتمثل وسائل التحري المناسبة للعالم الافتراضي في الاختراق، التقصي تحت اسم مستعار، واعتراض المعطيات عن بعد. وقد قامت فرنسا بتعديل مجلة إجراءاتها الجزائية حتى تسمح لأعوان الضابطة العدلية المنتمين لمصلحة خاصة من القيام بعمليات، التقصي تحت اسم مستعار عندما تكون الجرائم مرتكبة باستعمال

(41) Charpenel Y, Op. Cit.

(42) تنص المادة (8) من القانون رقم 63 لسنة 2015 في شأن مكافحة جرائم تقنية المعلومات على أنه: «يعاقب بالحبس مدة لا تجاوز سبع سنوات وبغرامة لا تقل عن عشرة آلاف دينار ولا تجاوز ثلاثين ألف دينار أو بإحدى هاتين العقوبتين، كل من أنشأ موقعاً أو نشر معلومات باستخدام الشبكة المعلوماتية أو بأي وسيلة من وسائل تقنية المعلومات المنصوص عليها في هذا القانون، بقصد الاتجار بالبشر أو تسهيل التعامل فيهم، أو ترويج المخدرات أو المؤثرات العقلية وما في حكمها، أو تسهيل ذلك في غير الأحوال المصرح بها قانوناً».

وسائل اتصال معلوماتي[43]. ويسمح هذا النص القانوني الجديد بالمشاركة في محادثات تحت اسم مستعار وبشراء والاحتفاظ بمحتويات غير شرعية دون الحصول على إذن قضائي أو تحديد مدة قصوى لهذه العمليات. وتكون بالتالي هذه الوسيلة الافتراضية أقل تعقيداً من عملية الاختراق "الجسدي" التي تستوجب الحصول على إذن قضائي وتكون محددة في الزمن[44]. ولهذه التقنية أهمية كبرى إذ إن لها بعداً وقائياً، فإمكانية أن يكون المتحدث على الإنترنت رجل أمن متخفياً من شأنها أن تردع محاولة ارتكاب الجرائم، وتستعمل هذه التقنية مثلاً للكشف عن مرتكبي الاعتداءات الجنسية ضد الأطفال.

21. بالإضافة إلى ذلك يسمح التقاط البيانات للمحققين المؤهلين، وبإذن قضائي، من الاستيلاء على البيانات عن بُعد من خلال إدخال برامج ضارة Malware (أو حصان طروادة)، مما يسمح للمحقق برؤية وتسجيل، عن بعد، بيانات الكمبيوتر، كما يتم عرضها على جهاز الكمبيوتر، حتى عندما لا يتم تخزين البيانات على الجهاز، وهذا يعني أن المحقق يرى كل ما يظهر على شاشة الجاني ويسجل ضربات المفاتيح، وفي هذه الحالة، فإن برنامج "تور TOR" لم يعد يسمح بإخفاء أنشطة الجاني[45].

كما تسمح مجلة الجمارك الفرنسية في مادتها عدد (67) مكرر1–لأعوان الأمن والجمارك بالقيام بشراء الأسلحة لإثبات الجرائم المتعلقة بالأسلحة والمتفجرات[46].

22. أما في الولايات المتحدة الأمريكية، فإن أجهزة الأمن على غرار مكتب التحقيقات الفيدرالي (FBI) تستعمل برامج تجسس وقرصنة بعد الحصول على إذن قضائي. وقد تمكن الـ FBI من حجز موقع يحمل صوراً إباحية لأطفال، ثم وضع المحققون برنامجاً ضاراً (Malware) في هذا الموقع يتسرب إلى جميع أجهزة الكمبيوتر التي تقوم بالدخول إليه. ويجبر هذا البرنامج جهاز الكمبيوتر على إعطاء هويته الحقيقية (أي عنوان IP الحقيقي) ويصبح بالتالي سهلاً بالنسبة للمحققين أن يجدوا مالك

(43) الفصل (706–87–1) جديد من مجلة الإجراءات الجزائية الفرنسية.

(44) الفصل (706–81) من مجلة الإجراءات الجزائية الفرنسية. في تونس يسمح الفصل (57) من القانون الأساسي عدد 26 لسنة 2015 مؤرخ في 7 أوت/أغسطس 2015 يتعلق بمكافحة الإرهاب ومنع غسيل الأموال في الحالات التي تقتضيها ضرورة البحث اللجوء إلى الاختراق بواسطة عون أمن متخف أو مخبر معتمد من قبل مأموري الضابطة العدلية المخول لهم معاينة الجرائم الإرهابية. ويباشر الاختراق بمقتضى قرار كتابي معلل من وكيل الجمهورية أو من قاضي التحقيق وتحت رقابته لمدة أقصاها أربعة أشهر قابلة للتمديد لنفس المدة بقرار معلل. ويمكن في أي وقت الرجوع في القرار المنصوص عليه بهذا الفصل.

(45) Quéméner (M), Enquêtes dans le Darkweb, Dalloz IP/IT, 2017, p.83.

(46) Charpenel (Y), Le Darkweb, un objet juridique parfaitement identifié: Le paradis, lo enfer», Dalloz, IP/IT, 2017, p.71.

جهاز الكمبيوتر بالاستناد على المعلومات التي يوفرها مزود خدمات الإنترنت. وفي حالة الموقع الذي تم حجزه في 2016/01 والذي كان يرتاده 215000 عضواً تمكنت السلطات من الحصول على عناوين إنترنت (IP) لنحو 1300 جهاز حاسوب، تم إثرها تحريك الدعوى ضد 137 شخصاً، وهو ما يؤكد نجاعة هذه الطرق الجديدة للتحريات[47].

كما تقوم السلطات في الدول الغربية بعمليات أمنية مشتركة تهدف إلى تحديد هوية وتعقب المعاملات الإجرامية على الإنترنت المظلم. وعلى سبيل المثال، فقد انخرط في عملية Hyperion عدد من أجهزة الشرطة في أستراليا، كندا، نيوزيلندا، المملكة المتحدة، والولايات المتحدة فيما يسمى بالـ"FELEG". وخلال عملية "هيبيريون"، اتصل عملاء مكتب التحقيقات الفيدرالي بأكثر من 150 فرداً يشتبه في شرائهم سلعاً غير مشروعة من أسواق مختلفة في الإنترنت المظلم، وقد اعترف بعض هؤلاء الأفراد بطلب مجموعة من العقاقير المخدرة وغير المشروعة عبر الإنترنت، بما في ذلك الهيروين والكوكايين والمورفين والكيتامين[48].

23. إلا أن هذه التحريات ولئن كانت ناجعة، فإن لها كلفة عالية، ولا شك أن تكاليف إثبات الأدلة التي يمكن اعتمادها أمام القضاء قد زادت زيادة كبيرة بسبب أساليب التحري الخاصة التي ينبغي حشدها[49].

كما لا يجب أن تقتصر مكافحة إجرام الإنترنت المظلم على استهداف مواقعه فقط، بل يجب أن تشهر السلطات بنقاط ضعفها، فإغلاق هذه المواقع ومقاضاة مديريها لئن كان أمراً ضرورياً فإنه ليست أمراً كافياً على المدى الطويل لمكافحة تجارة الإنترنت المظلم، لأنه تنشأ مواقع جديدة تأخذ أماكنها وترث حرفاءها. وقد كان لإغلاق سوقي (AlphaBay) و(darknet Hansa) في منتصف عام 2017 آثار مشابهة لإغلاق سوق Road Silk سنة 2013 حيث لم تضطرب السوق على الإنترنت المظلم إلا بصفة مؤقتة. وانتقل الحرفاء بصفة سريعة إلى التسوق في أسواق أخرى أصغر حجماً.

وفي اعتقادنا، فإنه ينبغي أن تقوم السلطات بإدخال الشك لدى هؤلاء المتعاملين بشأن سلامة المواقع وتقليص الشعور لديهم بإمكانية الإفلات من العقاب عن طريق كشف مخاطر ونقاط الضعف الخاصة بهذه المواقع علانية. وعلاوة على

(47) Quéméner M, Enquêtes dans le Darkweb, Dalloz, IP/IT, 2017, p.83.
(48) https:www.fbi.gov/news/stories/a-primer-on-darknet-marketplaces
(49) Charpenel Y, Le Darkweb, un objet juridique parfaitement identifié: Le paradis, l'enfer?, Dalloz, IP/IT, 2017, p.71.

ذلك، فإن إخفاء الهوية في هذه الأسواق يعطي بعض الغطاء على وجود الشرطة، ويسمح لها بالتفاعل مع المستخدمين، وبينما يشعر هؤلاء المستخدمون في كثير من الأحيان بالثقة والأمان لما يتسوقون على الإنترنت المظلم، فإن الوعي لديهم بإمكانية تعرضهم للملاحقة والعقاب قد يؤدي على نحو متزايد إلى إثنائهم عن مثل هذا الصنيع، وبالتالي تقليص إيرادات هذه الأسواق[50]. وقد اعتمدت المحاكم الأمريكية نهجاً متشدداً إزاء الجرائم المرتكبة على الإنترنت المظلم، إذ أيدت محكمة الاستئناف للولايات المتحدة الأمريكية قرار محكمة مقاطعة نيويورك الجنوبية بتسليط عقوبة السجن مدى الحياة على مؤسس سوق طريق الحرير Road Silk، وذلك بالرغم من إقرار محكمة الاستئناف بشدة هذه العقوبة وطابعها الاستثنائي[51].

24 . مما لا شك فيه أن زجر الإجرام الذي يتطور ويترعرع على الإنترنت المظلم أمر صعب ومكلف، وهو ما يحيلنا على طرح سؤال جوهري: ألا يجب منع تحميل واستعمال برامج إخفاء الهوية من نوع "تور TOR»؟ في الواقع لا تخلو هذه الفرضية من الجاذبية، إذ إن برامج إخفاء الهوية هي بوابة الدخول للإنترنت المظلم وبمنعها يمنع الدخول لهذا الفضاء. وقد أغرت هذه الفرضية السلطات الفرنسية غداة الهجمات الإرهابية التي ضربت فرنسا، فاقترحت وزارة الداخلية منع اتصالات واي فاي (Wi–Fi) الحرة والمشتركة، إضافة إلى منع برامج إخفاء الهوية، وقد لاقى هذا الاقتراح معارضة شديدة تسببت في العدول عنه، كما أن المنع قد لا يكون ممكناً من الناحية العملية، لأنه حتى لو تم إغلاق برنامج «تور» ستظهر برامج أخرى لتأخذ مكانه[52].

وفي نفس الإطار أقر المشرع الإماراتي في المادة (9) من القانون الاتحادي رقم (5) لسنة 2012 بشأن مكافحة الجرائم الإلكترونية عقوبة السجن المؤقت والغرامة التي لا تقل عن خمسمائة ألف درهم، أو بإحدى هاتين العقوبتين، كل من تحايل على العنوان البروتوكولي للشبكة المعلوماتية باستخدام عنوان وهمي أو عنوان عائد للغير أو بأي وسيلة أخرى، وذلك بقصد ارتكاب جريمة أو الحيلولة دون

(50) Yaya J. Fanusie and Tom Robinson, "Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services", January 12, 2018, https://info.elliptic.co/whitepaper–fdd–bitcoin–laundering.

(51) United States v. Ulbricht, N° 15–1815–CR May 31, 2017. United States v. U – bricht, No. 15–1815–CR (2d Cir. Jan. 12, 2016), 2016 WL 158389.

(52) Jardine, Eric, The Dark Web Dilemma: Tor, Anonymity and Online Policing (September 30, 2015). Global Commission on Internet Governance Paper Series, No. 21. Available at SSRN: https://ssrn.com/abstract=2667711 or http://dx.doi.org/10.2139/ssrn.2667711.

اكتشافها[53]. وبالتالي فإن استعمال برنامج "تور" قصد ارتكاب جريمة أو الحيلولة دون اكتشافها فعل مُجرم في حد ذاته في دولة الإمارات. وفي الواقع قد يصعب عملياً تطبيق هذه المادة إذ يستوجب ذلك في مرحلة أولى تحديد هوية المبحر الذي يغير من عنوانه البروتوكولي، إضافة إلى إثبات انصراف نيته لارتكاب جريمة أو الحيلولة دون اكتشافها.

25. إن مكافحة الإنترنت المظلم لا يمكن أن تتم إلا بصفة عالمية وتستوجب تعزيز وسائل التعاون القضائي الدولي وتطوير التعاون بين أجهزة الشرطة في مختلف دول العالم[54]. كما يتعين منح المؤسسات القضائية وأجهزة الشرطة فرصة توفير التدريب الأولي الذي يتم تكييفه لجميع أولئك الذين لديهم مهارة لمحاربة تجاوزات الإنترنت المظلم، من أجل منحهم وسائل تضمن نجاعة ومصداقية عملهم، لأن عدم الوعي بالتحدي الذي تفرضه حقيقة الإنترنت المظلم يعني المخاطرة برؤية حكم القانون يتلاشى بسرعة في العالم الافتراضي[55]. وبما أن المال قوام الأعمال، فإن مكافحة هذه الجرائم لا يمكن أن تكون ناجعة دون فرض رقابة على استعمال العملات الافتراضية التي هي عملة التداول على الإنترنت المظلم.

الفرع الثاني

تقييد استعمال العملات الافتراضية

26. يوفر نمو العملات الافتراضية المشفرة والتقنيات المرتبطة بها فرصًا كبيرة للمؤسسات الاقتصادية لتطوير نماذج أعمال جديدة، وللحكومات لبناء أنظمة معلومات أكثر كفاءة وأمانًا، ولإدراج الملايين من الأشخاص الذين يفتقرون إلى سهولة الوصول إلى النظام المصرفي التقليدي. وتمثل بالتالي تقنية تشفير العملات Cryptocurrency وblockchain، مكسبًا اقتصاديًا واجتماعيًا محتملا[56].

(53) قانون اتحادي رقم 12 لسنة 2016 بتعديل المرسوم بقانون اتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات.

(54) Saenko (L), Le Darkweb: un nouveau défi pour le droit pénal contemporain, Dalloz, IP/IT, 2017, p.80.

(55) Charpenel)Y), Le Darkweb, un objet juridique parfaitement identifié : Le paradis, lOenfer, Dalloz, IP/IT, 2017, p.71.

(56) اعتبر محافظ البنك المركزي التونسي أن تكنولوجيا البلوكشاين Blockchain (التي تقوم عليها العملات الافتراضية) تمثل فرصة هامة لتطوير النظام المالي التونسي، انظر:
http//:www.businessnews.com.tn/Chedly-Ayari--La-Tunisie-pourrait-servir-de-laboratoire-pour-le-lancement-de-la-Blockchain.520,76103,3,-

وفي الوقت نفسه، فإن غسيل الأموال عبر هذه العملات الافتراضية المشفرة هو تقنية جديدة من تقنيات غسيل الأموال، فغاسلو الأموال يبحثون بصفة مستمرة عن طرق جديدة لإخفاء مصدر ووجهة أموالهم، ومن الواضح أن أولئك الذين يسعون إلى غسيل الأموال يرغبون في القيام بذلك دون الكشف عنهم أو دون مخالفة القوانين القائمة، لذلك فهم يستغلون الثغرات الموجودة في الأنظمة الحالية ويستكشفون كل الطرق الجديدة التي من شأنها إرباك السلطات المكلفة بإنفاذ القانون. إن المعاملات التي تتم عبر الحدود جذابة بالنسبة إليهم بسبب إمكانية خداع السلطات والاختفاء عنها. ونفس الشيء بالنسبة لوسائل الدفع الإلكترونية الناشئة التي تكون جذابة لأن هذه التقنيات الجديدة من الأرجح ألا تكون مفهومة جيداً من قبل السلطات[57]. ويمكن للمجرمين الانتفاع من مزايا المعاملات الدولية ووسائل الدفع الجديدة عن طريق تحويل الأموال عبر الإنترنت، إذ يوفر الإنترنت فرصاً هائلة للمجرمين لتحويل الأموال، مع جعل إمكانية مراقبة وتتبع هذه الأموال صعبة بالنسبة لسلطات إنفاذ القانون. ويُعد ظهور "البيتكوين" واحداً من أكثر التطورات إثارة لغاسلي الأموال في السنوات الأخيرة[58].

27. ويطرح الإجرام المرتكب بواسطة "البيتكوين" أو غيره من العملات الافتراضية إشكالية كيفية منع وزجر هذا السلوك. في بادئ الأمر لا بد من الإشارة إلى أن غسيل الأموال باستعمال العملات الافتراضية المشفرة من نوع "بيتكوين" مُجرَّم سواء أكان ذلك في الكويت أم في تونس. وفي الكويت يُجرم القانون رقم 63 لسنة 2015 في شأن مكافحة جرائم تقنية المعلومات، غسيل الأموال عن طريق الشبكة المعلوماتية أو باستخدام وسيلة من وسائل تقنية المعلومات إذ تنص المادة (9) منه على أنه: "يعاقب بالحبس مدة لا تجاوز عشر سنوات وبغرامة لا تقل عن عشرين ألف دينار ولا تجاوز خمسين ألف دينار أو بإحدى هاتين العقوبتين، كل من قام عن طريق الشبكة المعلوماتية أو باستخدام وسيلة من وسائل تقنية المعلومات، بغسيل أموال أو بتحويل أموال غير مشروعة أو بنقلها أو بتمويه أو بإخفاء مصدرها غير المشروع، أو قام باستخدامها أو اكتسابها أو حيازتها مع علمه بأنها مستمدة من مصدر غير مشروع، أو بتحويل الموارد أو الممتلكات مع علمه بمصدرها غير المشروع، وذلك بقصد إضفاء الصفة المشروعة على تلك الأموال".

(57) Robert Stokes, Anti–Money Laundering Regulation and Emerging Payment Technologies, Banking & Fin. Servs. Pol'y Rep., May 2013, at 1, 1.

(58) Christopher, Catherine Martin, Whack–a–Mole: Why Prosecuting Digital Cu – rency Exchanges Won○t Stop Online Laundering (2014). 18 Lewis & Clark L. Rev. 1 (2014). Available at SSRN: https://ssrn.com/abstract=2312787.

وقد احتوت هذه المادة على تعريف واسع / التي يتم بها تبييض الأموال أي: "عن طريق الشبكة المعلوماتية أو باستخدام وسيلة من وسائل تقنية المعلومات".

وقد عرفت المادة الأولى من قانون مكافحة جرائم تقنية المعلومات الكويتي وسيلة تقنية المعلومات بكونها أداة إلكترونية تشمل كل ما يتصل بتكنولوجيا المعلومات وبذي قدرات كهربائية أو رقمية أو مغناطيسية أو بصرية أو كهرومغناطيسية أو ضوئية أو وسائل أخرى مشابهة سلكية كانت أو لاسلكية وما قد يستحدث في هذا المجال، وهو تعريف يشمل العملات الافتراضية المشفرة التي هي وسيلة تتصل بتكنولوجيا المعلومات تعمل باستخدام شبكة الإنترنت. أما في تونس فلا يحتوي القانون على نصوص خاصة تتعلق بغسيل الأموال عبر تقنيات المعلومات، إلا أن القانون عدد 22 لسنة 2015 مؤرخ في 7 أوت/أغسطس 2015 المتعلق بمكافحة الإرهاب ومنع غسيل الأموال لم يحصر الوسائل التي يتم بها غسيل الأموال، إذ جرَّم هذه العملية مهما كانت الطرق المستعملة، مما يجعل غسيل الأموال باستعمال الإنترنت والمعلوماتية داخلاً في نطاق التجريم.

28. من الواضح أن التجريم وحده غير كاف، فتقنين وتعديل العملات الافتراضية ليس بالأمر الهين، وهو يستوجب تقنين مبادلات "البيتكوين"، وفرض رقابة على المؤسسات والأشخاص الذين يسهلون أو يمارسون هذه المعاملات. وقد يكون بالتالي من البديهي التساؤل إن كان لزاماً منع "البيتكوين" والعملات الافتراضية الأخرى لتفادي استعمالها في النشاطات الإجرامية؟

لقد تم طرح هذه الإمكانية في السنوات الأولى لبروز هذه العملة من قبل السلطات في عدة دول[59]، إلا أنه بعد أشهر من الأعمال والاستشارات استقر الرأي على أن العملات الافتراضية لها عدد من المزايا بالنسبة للنظام المالي[60]، كما أن المنع التام أمر صعب التصور[61].

في الواقع إن منع العملات الافتراضية قد لا يكون ممكناً ولا محبذاً، وذلك لأن هذه العملات لا تعترف بالحدود، كما أن لها مزايا لا ينبغي التغاضي عنها، وبدلاً من

(59) طرح هذا السؤال في البرلمان الفرنسي، انظر:
E. Straumann, Question n, 51719 °JO, 11 mars 2014, p. 2243.

(60) Benjamin Lawsky, Superintendent du New York Department of Financial Se – vices: «Indeed, virtual currency could ultimately have a number of benefits for our financial system. It could force the traditional payments community to up its game in terms of the speed, affordability, and reliability of financial transactions», Wall Street Journal, 28 january 2014.

(61) Pierre Storrer, Crowdfunding, bitcoin: quelle régulation», D. 2014. P.832.

ذلك ينبغي فرض عدد من الالتزامات على نقاط التلاقي بين العملات الافتراضية والعملات القانونية أي منصات تبادل وصرف هذه العملات مع العملات المتداولة قانوناً (دولار، أورو، ين...).

يجب على السلطات المالية في جميع الدول أن تزيد من فرض مكافحة غسيل الأموال على منصات تبادل العملات ومواقع المقامرة عبر الإنترنت. وقد اعتبرت دراسة أن مفتاح مكافحة تبييض الأموال هو قيام السلطات المالية بالتحقيق في ممارسات مكافحة غسيل الأموال ومعرفة عميلك التي تعد ضعيفة ومحدودة من قبل الشركات التي تقوم بتحويل الأموال دون ترخيص أو امتثال لقواعد ترتيبية[62].

29. وقد تولت فرنسا مثلاً إجراء تعديلات في قوانينها قصد تعزيز واجبات التصريح بالشبهات المحمولة على الوسطاء في مجال العملات الإلكترونية، إذ تولى الأمر عدد 1523–2016 المؤرخ في 10/11/2018 المتعلق بمكافحة غسيل الأموال وتمويل الإرهاب تنقيح المجلة المالية والنقدية لتعزيز واجبات التصريح بالشبهة للوسطاء في مجال العملات الإلكترونية. كما اتفقت دول الاتحاد الأوروبي على تعزيز مكافحة غسيل الأموال و تمويل الإرهاب على منصات تبادل «البيتكوين» والعملات الافتراضية الأخرى[63].

30. في الأخير لا بد من الإشارة إلى أن «البيتكوين» هو العملة الافتراضية الأولى ولكنه ليس العملة الافتراضية الوحيدة، ففي السنوات الأخيرة، تم ابتكار عملات افتراضية مشفرة جديدة، مثل «زكاش Zcash ومونيرو Monero وداش Dash[64]، وهي عملات لها ميزات للخصوصية متطورة تجعل مراقبتها وتعقبها أكثر صعوبة،

(62) Yaya J. Fanusie and Tom Robinson, "Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services", January 12, 2018, https://info.elliptic.co/whitepaper-fdd-bitcoin-laundering.

(63) «Les Etats ne pourront pas réguler le bitcoin sans les autres, dit un responsable de la banque centrale allemande», 152018,/01/ http://www.businessinsider.fr/bundesbank-conseille-reglementation-mondiale-bitcoin

(64) دور الـ Monero و Ether كعملة تبادل بصدد النمو في أسواق الإنترنت المظلم، وهو ما يؤكد قدرة المجرمين على التأقلم وعلى استخدام أحدث التقنيات، انظر:

Andy Greenberg" ,Monero ,the drug dealer□s cryptocurrency of choice ,is on fire," 25/01/2017

https://www.wired.com/2017/01/monero-drug-dealers-cryptocurrency-choice-fire/

Rachel Rose O'Leary, "Europol Warns Zcash, Monero and Ether Playing Growing Role in Cybercrime," CoinDesk, October 3, 2017. https://www.coindesk.com/e-ropol-warns-zcash-monero-and-ether-playing-growing-role-in-cybercrime/.

ولا بد بالتالي من الوعي بهذا الخطر وتطوير القواعد القانونية والتقنيات الكفيلة بمراقبة المعاملات التي تتم بواسطة هذه العملات، ومن المؤكد أن رفع هذا التحدي ليس بالأمر الهين، ويستوجب من رجال القانون اكتساب الخبرات التقنية اللازمة لمكافحة الاستعمال غير القانوني لهذه العملات، كما ينبغي على المشرع والسلطات المالية الوعي بمخاطر بروز عملات افتراضية مشفرة تمكن أكثر فأكثر من التخفي وإخفاء الهوية[65]. وبالطبع فإن كل تقنين للعملات الافتراضية يجب أن يتم على الصعيد العالمي؛ لأن القواعد الوطنية والإقليمية قد لا تجد مجالاً للتطبيق في عالم افتراضي لا يعترف بالحدود.

(65) Yaya J. Fanusie and Tom Robinson, Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services, January 12, 2018, https://info.elliptic.co/whitepaper–fdd–bitcoin–laundering.

الخاتمة:

31. إن خصوصيات الإنترنت المظلم والعملات الافتراضية تجعل منها أدوات مثالية بالنسبة للمجرمين والمنظمات الإجرامية، فاستخدام الإنترنت المظلم يسمح لهؤلاء بالانخراط في أعمال إجرامية سرية صعبة الكشف والزجر، ويسمح لهم بالنشاط على نطاق واسع يشمل جميع دول العالم، كما أن سهولة استعمال برمجيات إخفاء الهوية وصعوبة الكشف عن هذه الجرائم تبرز التحدي الذي تواجهه السلطات.

وبما أن أنشطة هؤلاء المجرمين عابرة للحدود، فإن مكافحة الإنترنت المظلم لا يمكن أن تتم إلا بصفة عالمية، وتستوجب تعزيز وسائل التعاون القضائي الدولي وتطوير التعاون بين أجهزة الشرطة في مختلف دول العالم. إن تجريم الأفعال وحده لا يكفي لضمان زجر فعال للجرائم التي ترتكب على الإنترنت المظلم، إذ يجب تبني وتعزيز وتطوير وسائل التقصي المناسبة لهذا الفضاء، وذلك في ظل قصور وسائل التحري التقليدية. وتتمثل وسائل التحري المناسبة للعالم الافتراضي في الاختراق، التقصي تحت اسم مستعار واعتراض المعطيات عن بعد.

32. وبالإضافة إلى ما سبق ذكره، فإن تقليص الإجرام النابع عن الإنترنت المظلم يفترض مكافحة مصادر تمويله، وهو ما يطرح إشكالية مراقبة تداول العملات الافتراضية حتى لا يتم استعمالها لأغراض إجرامية، وفي هذا الصدد اتخذت السلطات التعديلية في الصين قراراً بفرض تضييقات على العملات الافتراضية، وقامت بغلق عدد من منصات تبادلها. كما تدرس كوريا الجنوبية منع تداول هذه العملات(66). عملياً فإن هذا المنع الكلي قد لا يكون ممكناً أو ناجعاً خاصة إذا لم يتم اتخاذه في إطار دولي.

33. إن رفع هذه التحديات الجديدة النابعة عن التطور التكنولوجي يفرض على الباحثين والأكاديميين في مختلف المجالات وعلى السلطات المكلفة بإنفاذ القانون أن يدرسوا هذه الظواهر وأن يقوموا بصياغة إطار قانوني وتنظيمي يسمح ببسط سلطة القانون على الإنترنت المظلم وبمراقبة استخدام العملات الافتراضية المشفرة.

(66) «Les Etats ne pourront pas réguler le bitcoin sans les autres, dit un responsable de la banque centrale allemande», 152018, /01/ http: //www.businessinsider.fr/bundesbank-conseille-reglementation-mondiale-bitcoin.

المراجع:

1- Ouvrages spécialisés :

- Quémener et Ferry، Cybercriminalité: défi mondial et réponses، 2007، Economica.
- Stokes (R)، Anti-Money Laundering Regulation and Emerging Payment Technologies، Banking & Fin. Servs. Polly Rep.، May 2013، at 1، 1.

2- Articles :

- Bal (A)، Bitcoin and Money Laundering، http://www.offtax.com/articles/bitcoin-and-money-laundering.php#.VgFN1rVtJ-0.twitter.
- Charpenel)Y)، Le Darkweb، un objet juridique parfaitement identifié Le paradis، l'enfer?، Dalloz IP/IT 2017.
- Christopher، Catherine Martin، Whack-a-Mole: Why Prosecuting Digital Currency Exchanges Won>t Stop Online Laundering (2014). 18 Lewis & Clark L. Rev. 1 (2014). Available at SSRN: https://ssrn.com/abstract=2312787.
- De Maison Rouge (O)، Darkweb: plongée en eaux troubles، Dalloz، IP/IT، 2017.
- Ghappour (A)، Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web، Stanford Law Review، Vol. 69، Issue 4، April 2017.
- Jardine، Eric، The Dark Web Dilemma: Tor، Anonymity and Online Policing (September 30، 2015). Global Commission on Internet Governance Paper Series، No. 21.
- Marain (G)، Le bitcoin à l'épreuve de la monnaie، AJ contrat 2017.
- Peter Rudegeair and Akane Otani، Bitcoin Mania: Even Grandma Wants In on the Action، The Wall Street Journal، November 29، 2017. (https://www.wsj.com/articles/bitcoin-mania-even-grandma-wants-in-on-the-action-1511996653).
- Petit (A)، Visite guidée du Darkweb cybercriminel، Dalloz، IP/IT، 2017.
- Quéméner (M)، Enquêtes dans le Darkweb، Dalloz، IP/IT، 2017.
- Rudesill، Dakota S. and Caverlee، James and Sui، Daniel، The Deep Web and the Darknet: A Look Inside the Internet's Massive Black Box، October 20، 2015، Woodrow Wilson International Center for Scholars،

STIP 03، October 2015; Ohio State Public Law Working Paper No. 314.
- Saenko (L)، Le Darkweb: un nouveau défi pour le droit pénal contemporain، Dalloz، IP/IT، 2017.
- Samuel Gibbs، Man buys $27 of bitcoin، forgets about them، finds they're now worth $886k، The Guardian (UK)، December 8، 2015. (https://www.theguardian.com/technology/2015/dec/09/bitcoin-forgotten-currency-norway-oslo-home).
- Storrer (P)، Crowdfunding، bitcoin: quelle régulation?، D. 2014.
- Yaya J. Fanusie and Tom Robinson، Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services، January 12، 2018، https://info.elliptic.co/whitepaper-fdd-bitcoin-laundering.

3- Reports :

- Drug Enforcement Administration، 2017 National Drug Threat Assessment، https://www.dea.gov/docs/DIR-040-17_2017-NDTA.pdf.
- Financial Action Task Force (FATF) (2015)، Emerging Terrorist Financing Risks، FATF، Paris www.fatf-gafi.org/publications/methodsandtrends/documents/emerging-terrorist-financing-risks.html.
- Tracfin، Tendances et analyse des risques de blanchiment de capitaux et de financement du terrorisme en 2016، https://www.economie.gouv.fr/files/rapport-analyse-tracfin-2016.pdf.

المحتوى: