

المسئولية الجنائية الناشئة عن إساءة استخدام مواقع التواصل الاجتماعي

إعداد

د/ دينا عبدالعزيز فهمي

مقدمة

موضوع البحث:

الحمد لله رب العالمين الذي علم الإنسان ما لم يعلم، وأسبغ عليه نعمه ظاهرة وباطنة، فله الحمد في الأولى والآخرة، والصلاة والسلام على المبعوث رحمة للعالمين سيدنا محمد صلى الله عليه وسلم وعلى آله وأصحابه والتابعين لهم بإحسان إلى يوم الدين.

وبعد....

تعتبر تكنولوجيا الاتصالات والحاسب الآلي ثورة حقيقية في ميدان الاتصال والمعلومات، وأدت هذه الثورة إلى تراكم مدهل في المعرفة وحصيلة هائلة في المعلومات، غير أن هذه الابتكارات أفرزت جرائم جديدة غير معتادة عكست هذا الواقع، واستخدمت أدواته واتصفت بسماته، حتى إنها اقترنت باسمه فأطلق عليها "جرائم تقنية المعلومات" تناغماً مع مصطلح "عصر تقنية المعلومات"، ومن أبرز الأضرار التي تلحق بالمجتمع نتيجة ذلك استغلال مواقع التواصل الاجتماعي عبر الإنترنت ليس في أغراض الصداقة وتبادل المعلومات فحسب، وإنما في ارتكاب جرائم أيضاً، الأمر الذي يترتب عليه مخاطر اجتماعية وأمنية تصل إلى حد تهديد أمن الدولة.

وقد شهدت تكنولوجيا الاتصالات والمعلومات تطورات سريعة وتأثيرات مباشرة للثورة الرقمية على نمط الحياة⁽¹⁾، ويمكن تعريف تكنولوجيا المعلومات بأنها جميع أنواع التكنولوجيا المستخدمة في تشغيل ونقل وتخزين المعلومات في شكل إلكتروني، وتشمل تكنولوجيا الحاسبات الآلية ووسائل الاتصال، وأجهزة الفاكس وغيرها من المعدات التي تستخدم في الاتصالات.

وإذا كانت مواقع التواصل الاجتماعي توفر الجهد والوقت والمال في جمع المعلومات، فمن خلالها يمكن التوصل إلى جميع أنواع المعلومات الشخصية الخاصة بالفرد، وهذا يمثل فرصة حقيقية في جمع الاستدلالات عن الجرائم، فمن خلال تحليل محتوى الشبكات يمكن تحديد العلاقة بين المشتبه فيهم، والجرائم الناشئة عن استخدام مواقع التواصل الاجتماعي.

ونظرًا لتغير طبيعة الجرائم خلال السنوات الأخيرة واعتمادها على التقنيات الحديثة والفضاء الإلكتروني والمعلوماتي، أصبح من الضروري وضع الأطر القانونية التي تكفل حماية كل ما يهدد الدولة في هذا الشأن.

حيث يتم استخدام مواقع التواصل الاجتماعي، من قبل الإرهابيين وعصابات الجريمة المنظمة - وهو اتجاه لم يؤدِّ إلى تطوير أشكال جديدة من النشاط

(1) Denis Baresch: Sécurité et confiance dans la communication électronique - pour une approche européenne, Revue du Marché commun et de l'Union européenne, N° 420 du 10/07/1998, p.437.

الإجرامي فحسب، بل إلى "عولمة" الجريمة وظهور أنماط جديدة من الصراع "الاقتراضي"، تكون شبكة الإنترنت ساحة معركته، ومواقع التواصل الاجتماعي سلاحه، والدول والمواطنون مقاتليه.

حيث إن المرحلة الحالية التي تمر بها البلاد فاصلة في تاريخها الحديث وتحتشد فيها الجهود وتتضافر فيها القوى لخوض معركة التقدم نحو المستقبل الأفضل والشعور بالأمن والأمان الذي يصبو إليه جموع المصريين، ولعل أبرز ما نواجهه في هذه المرحلة من التقدم والتنمية هي جرائم تقنية المعلومات والجريمة الإلكترونية التي تهدف إلى تدمير كيان المجتمع وتعصف بأمنه واستقراره وتعوق مسيرة التقدم والازدهار، لذا كان لزاماً أن نسارع في مواجهة هذا الخطر الداهم وإنقاذ مواطنينا من تغييب عقولهم حتى يترسخ للبلاد أمنها واستقرارها ويتاح مناخ أفضل لمواصلة الجهود نحو الإصلاح والتنمية والتطور في نطاق الدستور والقانون.

وقد انضمت جمهورية مصر العربية في عام 2014 إلى الاتفاقية العربية لمكافحة جرائم تقنية المعلومات⁽¹⁾، وصدر في مصر قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018⁽²⁾، كما وضع المشرع الفرنسي العديد من النصوص

(1) الجريدة الرسمية، العدد 46، 13 نوفمبر 2014، قرار رئيس جمهورية مصر العربية رقم 276 لسنة 2014 بشأن الموافقة على انضمام جمهورية مصر العربية إلى الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، الموقعة في القاهرة بتاريخ 2010/12/21.

(2) الجريدة الرسمية، العدد 32 مكرر(ج)، 14 أغسطس 2018، قانون رقم 72 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات.

لمكافحة جرائم تقنية المعلومات, والقانون الإماراتي لمكافحة جرائم تقنية المعلومات في المرسوم بقانون اتحادي رقم (5) لسنة 2012 في شأن تقنية المعلومات⁽¹⁾ ووضع قواعد تحد من مخاطر هذه المواقع, والقانون الكويتي رقم (63) لسنة 2015 في شأن مكافحة جرائم تقنية المعلومات⁽²⁾.

أهمية البحث:

أدى تطور مواقع التواصل الاجتماعي، وزيادة عدد الأفراد الذين يستخدمون هذه المواقع إلى تفاقم المشكلات القانونية، الأمر الذي يتعين على المشرع المصري وضع قانون لمواجهة مخاطر إساءة استخدام هذه المواقع، ولاسيما أن التحديات الناشئة عن سوء استخدام مواقع التواصل الاجتماعي لا تقف عند حد المساس بالحقوق الخاصة بالأفراد فحسب، بل يمتد تأثيرها إلى ما يهدد سلامة وأمن الدولة، ويلاحظ في الآونة الأخيرة أنه يتم استغلال هذه المواقع في إثارة الشعوب وإحداث فوضى سياسية.

تعتبر مواقع التواصل الاجتماعي اليوم بمثابة وسائل إعلامية، تعرف بالإعلام الجديد، تعد اليوم أهم السمات البارزة، التي يستطيع الشخص استخدامها وكتابة

(1) المرسوم بقانون اتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات.

(2) القانون رقم (63) لسنة 2015 في شأن مكافحة جرائم تقنية المعلومات، صدر بقصر السيف في 20 رمضان 1436 هـ - الموافق 7 يوليو 2015 م.

منشوراته ونشر مقاطعه الصوتية أو المرئية وهو في أي مكان في العالم, وقد نتج عن ذلك تجاوزات, ومن ثم يتعين التصدي لها.

■ تحديد المسؤولية الجنائية في جرائم النشر الإلكتروني التي ترتكب من خلال مواقع التواصل الاجتماعي؛ فهل المسئول باعتباره يؤدي دوراً رئيسياً في تنظيم المعلومات هو مزود خدمات الاستضافة وتخزينها على شبكة الإنترنت، أو كونه مباشر خدمات تقنية تتمثل في توصيل خدمة الاتصال ولا علاقة له بالبيانات، أو المعلومات، التي يتم نشرها على هذه المواقع، أم هو الناشر الإلكتروني باعتباره محرر الموقع ويقوم بصياغة المعلومات، ويتحكم في البيانات التي يتم نشرها على صفحات مواقع التواصل الاجتماعي؟ وقد يجتمع الأمران معاً بأن يصبح منشئ الموقع هو ذاته الذي أنيط به تحرير المحتوى، فمن المسئول عن المعلومات الواردة في ذلك المحتوى إذا تضمنت الإساءة إلى مستخدمي تلك المواقع؟

■ ظهور نوع جديد من جرائم الإرهاب وهي جرائم الإرهاب عبر مواقع التواصل الاجتماعي, والتي تتم من خلال استخدام الإنترنت وتطبيقاته المختلفة, وهي جرائم تتسم بالخطورة لسهولة ارتكابها, والتخطيط لها وتدريب الجناة ونشر معلوماتها, وسرعة الاتصال فيما بينها, نظراً لاستفادتها من خدمة تقنية المعلومات وتطبيقاتها.

▪ خطورة جريمة الإرهاب عبر مواقع التواصل الاجتماعي, حيث لم تعد التكنولوجيا وحدها قادرة على حماية الأفراد من جرائم الإرهاب والتنظيم الإرهابي عبر مواقع التواصل الاجتماعي, والتي تترك آثار وأضرار تمس المجتمع.

▪ صدور القانون رقم (175) لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات, وبالتالي أصبح هذا الموضوع حديث الساعة, فبعد أن كانت مشكلة جرائم تقنية المعلومات مثارة بالطبع قبل صدور القانون, إلا أنها أصبحت أكثر إثارة بعد صدوره لما كان لهذا القانون إحداث زلزال في أثره في مكافحة تلك الجرائم, فضلاً عما أعتري هذا القانون من الخلل والقصور في بعض مواضعه والتي سنعرض كل منها في حينه في هذا البحث آملين أن نسد هذا النقص والقصور من خلال المقارنة بالقوانين الأخرى ومن خلال رأينا المتواضع, ولذلك أتمنى أن يكون لي شرف المحاولة لمناقشة هذا القانون مع إضفاء الجديد من الاقتراحات على أن يحذوني الأمل أن يأخذ بها المشرع المصري مستقبلاً عند إجراء أي تعديل قد يطراً على هذا القانون, بما يجعل هذا القانون في مصاف القوانين المنظمة لمكافحة جرائم تقنية المعلومات.

منهج البحث:

بسبب حداثة قانون مكافحة جرائم تقنية المعلومات في مصر وقلة الأحكام القضائية فيه, ولكي نصل إلى الأهداف المرجوة من هذا البحث اعتمدت على المنهج

المقارن, وكانت المقارنة بين بعض التشريعات والقانون المصري للوصول إلى ما يكون مناسباً لسد بعض الثغرات في القانون لنخطو خطاها ونسير على دربها. ونظراً لعدم وجود قانون في مصر ينظم استخدام مواقع التواصل الاجتماعي صراحة, اتبعت في هذا البحث المنهج التأصيلي في تأصيل فكرة النظام القانوني لمواقع التواصل الاجتماعي, ببيان ماهيتها وأنواعها ونصوص تجريم إساءة استخدامها في القانون الفرنسي وغيره من القوانين, هذا بالإضافة إلى الاستعانة بالمنهج التحليلي في تحليل نصوص التشريعات الأجنبية, وذلك للتوصل لحل المشكلات التي تنتج عن موضوع البحث, هذا بالإضافة إلى الاستعانة بالمنهج المقارن بالمقارنة بين بعض التشريعات.

خطة البحث:

المبحث الأول: ماهية مواقع التواصل الاجتماعي.

المبحث الثاني: نطاق المسؤولية الجنائية لإساءة استخدام مواقع التواصل الاجتماعي.

المبحث الأول

ماهية مواقع التواصل الاجتماعي

تمهيد وتقسيم:

انتشرت مواقع التواصل الاجتماعي ووسائل الاتصالات وأشهرها الهاتف المحمول، ومع تنوع وسائل الاتصالات، وكذلك البرامج الإلكترونية المختلفة حيث تستطيع من خلالها ابتكار كل ما هو جديد، ومنها برامج تحرير الصور وأشهرها برنامج الفوتوشوب التي يستطيع الشخص من خلاله تركيب ودمج الصور مع أخرى ومن ثم نشرها على مواقع التواصل الاجتماعي المختلفة وأشهرها «تويتر» و«فيسبوك»، بالإضافة إلى بعض البرامج الأخرى كبرامج المشاركة حيث يقوم مستخدمو هذه البرامج بنشر الصور والفيديوهات ليشاهدها الجميع في كل أنحاء العالم، وما يسبب ذلك ضرر كبير خاصة إذا كانت هذه المحتويات تضر بأخرين أو تسيء إليهم.

بالإضافة إلى ذلك فإن مواقع التواصل الاجتماعي وهذه البرامج أصبحت لا تقتصر على الحاسب الآلي، بل أصبح استخدامها متاحاً على الهواتف المحمولة بإمكانياتها الحديثة وما تملكه من إمكانيات جعلت من جهاز الهاتف المحمول حاسبا آليا محمولا يستطيع من خلاله الأفراد استخدام هذه البرامج، وتحميل المواقع الإباحية ونشرها، بل أن هناك برامج تستخدم على الهاتف اخطر من برامج الحاسب الآلي، مثل برنامج الواتس أب الذي تستطيع من خلاله إرسال صور أو فيديوهات أو روابط تستطيع إرساله لأي شخص من خلال رقم هاتفه، ولتطور الحاسب الآلي وصغر حجمه شيئاً فشيئاً حتى وصل إلى الآيباد والتابلت،

ويعتبران بمثابة هاتف محمول كبير الحجم مما جعله سهل التنقل به وكذلك يكثر استعماله، مما سهل على أصحاب النفوس المريضة الذين أصبحت هذه الأمور هواية لديهم، فالعبث به أشكال كثيرة من التصرفات مثل القذف السبب والتشهير وغيره من التصرفات السيئة والمعاقبة قانوناً.

وتمثل مواقع التواصل الاجتماعي ثورة رقمية نتيجة استخدامها في نشر المعلومات، فالمستخدم يمكن له نشر برامج، أو مؤلفات على صفحات الويب، وإبرام صفقات تجارية، والتواصل مع أقاربه وأصدقائه، الأمر الذي جعل هذه المواقع ذات طبيعة عالمية.

ويقتضي التواصل الاجتماعي عبر هذه الشبكات وجود أجهزة مترابطة تستخدم لتدفق المعلومات، وعليه فالإنترنت هو السبب الرئيسي في ظهور مواقع التواصل الاجتماعي، وتحويل المستخدم السلبي إلى مستخدم نشط، وقادر على إنشاء معلومات ومحتوى، والتفاعل مع الآخرين⁽¹⁾.

أصبحت مواقع التواصل الاجتماعي اليوم إحدى المحطات المهمة في تطور العمل الإعلامي⁽²⁾، فضلاً عن توسيع رقعة الجمهور، وتجاوز الحدود المكانية، كما كان ظهور شبكة الإنترنت بمثابة ثورة غير مسبوقة في مجال وسائل الاتصال

(1) Géraldine Péronne & Emmanuel Daoud: Discriminations et réseaux sociaux, AJ Pénal, N° 12 du 11/12/2014, p.570.

(2) Sébastien Defix: Réseaux sociaux et règles de propagande électorale, AJ Collectivités Territoriales, N° 12 du 16/12/2014, p.580.

والمعلومات, بما أتاحتها من حرية وسرعة متابعة الحدث على مدار الساعة, وبما قدمته من خدمات متعددة من مواقع ومنشآت وتصفح, حيث أدى ذلك إلى زيادة دور شبكات التواصل الاجتماعي, باعتبارها وسائل حرة للتعبير والتفاعل والتواصل بين أفراد المجتمع.

المطلب الأول: مفهوم مواقع التواصل الاجتماعي.

المطلب الثاني: أهمية مواقع التواصل الاجتماعي.

المطلب الأول

مفهوم مواقع التواصل الاجتماعي

تمهيد وتقسيم:

تقوم فكرة مواقع التواصل الاجتماعي على جمع بيانات الأعضاء المشاركين في هذه المواقع، ويتم نشر البيانات علنا حتى يتجمع الأعضاء ذوو المصالح المشتركة والذين يبحثون عن ملفات أو صور لتسهيل الحياة الاجتماعية بين الأفراد، وبناء وتفعيل المجتمعات على شبكة الإنترنت.

فمواقع التواصل الاجتماعي هي التواصل بين الأفراد وجماعات المستخدمين، وتمكنهم من التواصل وتبادل الآراء والأفكار والمعلومات والملفات والصور والفيديو بين الأفراد المستخدمين لها في أي وقت يشاءون وفي أي مكان من العالم، واكتسبت اسمها الاجتماعي لتصبح وسيلة تعبيرية لدى الأفراد⁽¹⁾.

ونتناول في هذا المطلب إلى تعريف مواقع التواصل الاجتماعي، ثم بيان أنواعه على النحو التالي:

الفرع الأول: تعريف مواقع التواصل الاجتماعي.

(1) Nikita Barman: Legal Implications of Cyber Crimes on Social Networking Websites, International Journal of Scientific and Research Publications, Volume 5, Issue 12, December 2015 , p.315.

الفرع الثاني: صور مواقع التواصل الاجتماعي.

الفرع الثالث: خصائص مواقع التواصل الاجتماعي.

الفرع الأول

تعريف مواقع التواصل الاجتماعي

يُطلق على مواقع التواصل الاجتماعي باللغة الإنجليزية «social media» لكن هذا المصطلح المتعارف عليه كما نجد مصطلح «social net-work» أي الترابط الشبكي الاجتماعي والمصطلح العربي "مواقع التواصل الاجتماعي" أدق من ناحية الوصف.

أولاً: التعريف الفقهي لمواقع التواصل الاجتماعي:

عرف اتجاه في الفقه مواقع التواصل الاجتماعي بأنها منظومة من الشبكات الإلكترونية التي تسمح للمشارك فيها بإنشاء موقع خاص به، ومن ثم ربطه عن طريق نظام اجتماعي إلكتروني مع أعضاء آخرين لديهم الاهتمامات والهوايات نفسها⁽¹⁾.

وعرفت أيضاً بأنها شبكات اجتماعية تفاعلية تتيح التواصل لمستخدميها في أي وقت وفي أي مكان في العالم، ظهرت على شبكة الإنترنت منذ سنوات وتمكنهم

(1) د/ زاهر راضي، استخدام مواقع التواصل الاجتماعي في العالم العربي، مجلة التربية، العدد 15، جامعة عمان الأهلية، عمان، 2003، ص23.

من التواصل المرئي والصوتي وتبادل الصور وغيرها من الإمكانيات التي توطد العلاقة الاجتماعية بينهم⁽¹⁾.

مواقع التواصل الاجتماعي هي عبارة عن مجموعة من مواقع الاتصال عبر الإنترنت، وهذه المواقع تكون مخصصة للتفاعل والتبادل الاجتماعي، بحيث تكون مفتوحة لجميع الناس لتبادل الحوار والآراء وكتابة ما يرغبون بمشاركته أو نشره مع الناس الآخرين من جميع أنحاء العالم⁽²⁾. وللاشتراك بهذه المواقع ليس عليك إلا التسجيل من خلال الإيميل بكل سهولة لتصبح أحد المشتركين بهذه الوسائل المختلفة، التي تفتح أمامك العالم.

ويمكننا تعريف مواقع التواصل الاجتماعي بأنها مواقع أسسها أفراد أو شركات تستهدف جمع الأقارب والأصدقاء والمعارف وزملاء الدراسة أو العمل في مكان واحد على صفحات الويب ليشاركوا في الآراء والاهتمامات والتعليقات والأخبار وتكوين صداقات جديدة.

(2) عبد الرزاق محمد الدليمي، الإعلام الجديد والصحافة الإلكترونية، دار وائل للنشر، الطبعة الأولى، الأردن، 2011، ص 183.

(2) Emilie Bailly & Emmanuel Daoud: Cybercriminalité et réseaux sociaux: la réponse pénale, AJ Pénal, N° 05 du 14/05/2012, p.252.

ثانياً: التعريف القانوني لمواقع التواصل الاجتماعي:

عرف المشرع المصري في القانون رقم 175 لسنة 2018 الموقع بأنه نطاق أو مكان افتراضي له عنوان محدد على شبكة معلوماتية⁽¹⁾.

وعرّف المشرع الفرنسي التواصل الاجتماعي عبر شبكة الإنترنت في المادة الرابعة من القانون رقم 575 - 2004 الصادر 21 يونيو 2004⁽²⁾ بأنه بروتوكول اتصال مفتوح، أو ربط بيانات وتبادلها بأي شكل يصل إلى الجمهور دون قيد على أي محتوى تبادلي من قبل مقدمي الخدمات التقنية⁽³⁾.

عرف القانون الإماراتي رقم (5) لسنة 2012 الموقع الإلكتروني بأنه مكان إتاحة المعلومات الإلكترونية على الشبكة المعلوماتية، ومنها مواقع التواصل الاجتماعي، والصفحات الشخصية والمدونات⁽⁴⁾.

(1) المادة الأولى من القانون رقم 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات.

(2) JORF n°0143 du 22 juin 2004 page 11168, texte n° 2, Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.

(3) - "Article 4 En savoir plus sur cet article.

On entend par standard ouvert tout protocole de communication, d'interconnexion ou d'échange et tout format de données interopérable et dont les spécifications techniques sont publiques et sans restriction
".d'accès ni de mise en oeuvre

(4) المادة الأولى من القانون الإماراتي.

كما عرف القانون الكويتي رقم (63) لسنة 2015 الموقع بأنه مكان إتاحة المعلومات على الشبكة المعلوماتية من خلال عنوان محدد. وإلكتروني بأنه كل ما يتصل بتكنولوجيا المعلومات وذو قدرات كهربائية أو رقمية أو مغناطيسية أو بصرية أو كهرومغناطيسية أو وسائل أخرى مشابهه سلكية أو لا سلكية وما قد يستحدث من تقنيات في هذا المجال.

نرى أن المشرعين الفرنسي الإماراتي قد أحسنا صنعاً عند وضعهما لتعريف المواقع الإلكترونية، حيث إنه نص على اعتبار مواقع التواصل الاجتماعي أحد المواقع الإلكترونية، وذلك ما أغفله المشرع المصري والكويتي.

مواقع التواصل الاجتماعي هي المواقع على شبكة الإنترنت تسمى (réseaux sociaux) الشبكات الاجتماعية التي تتيح التواصل بين مستخدميها في بيئة مجتمع افتراضي يجمعهم وفقاً لاهتماماتهم أو انتماءاتهم الاجتماعية والثقافية، بحيث يتم ذلك عن طريق التواصل المباشر كإرسال الرسائل أو الصور أو مقاطع الفيديو وغيرها، ومشاركة الآخرين والتعرف على أخبارهم⁽¹⁾.

فالشبكات الاجتماعية هي مجموعة من المواقع على شبكة الإنترنت، تتيح التواصل بين الأفراد في بيئة مجتمع افتراضي يجمعهم حسب مجموعات اهتمام أو شبكات

(1) Sophie Prétot: L'ami des réseaux sociaux: précisions sur l'appréhension juridique de la communauté virtuelle, Dalloz actualité, 19 janvier 2017.

انتماء (بلد، جامعة، مدرسة، شركة... إلخ)، كل ذلك يتم عن طريق خدمات التواصل المباشر؛ مثل: إرسال الرسائل، أو الاطلاع على الملفات الشخصية للآخرين، ومعرفة أخبارهم ومعلوماتهم التي يقومون بعرضها.

فتطبيقات مواقع التواصل الاجتماعي على الإنترنت تتيح للمستخدمين أن يقوموا بتعريف ملامحهم الشخصية من خلال البيانات التي يدونها وعرض الصور، والاتصال بالأصدقاء الذين تعرفوا عليهم عن طريق الإنترنت أو في الواقع الحقيقي ومشاهدة البيانات الشخصية للآخرين.

ويمكننا تعريف مواقع التواصل الاجتماعي بأنها مجموعة من صفحات الويب التي تسهل التفاعل النشط بين الأعضاء المشتركين في مواقع التواصل الاجتماعي الموجودة بالفعل على شبكة الإنترنت، وتهدف إلى توفير مختلف وسائل الاهتمام التي تساعد الأعضاء على التفاعل بين بعضهم البعض.

ويمكن تعريفها بأنها مواقع إلكترونية اجتماعية على شبكة الإنترنت والركيزة الأساسية للإعلام الجديد أو البديل، التي تتيح للأفراد والجماعات التواصل فيما بينهم عبر الفضاء الافتراضي.

الفرع الثاني

صور مواقع التواصل الاجتماعي

أخذت شبكة الإنترنت تغزو كل مرافق الحياة، وأتاحت تواصل المواطنين بعضهم مع بعض، وتفاعلهم مع مختلف الأحداث والسياسات، إذ أحدثت التطورات التقنية الحديثة نقلة حقيقية في عالم الاتصال وربطت أجزاء العالم بفضائها الواسع، ومهدت الطريق لكافة المجتمعات في عالم الاتصال، للتقارب والتعارف وتبادل الآراء والأفكار والرغبات، وجعلت العالم كأنه قرية صغيرة.

وقد ساهمت التطورات المتلاحقة في شبكة الإنترنت في إيجاد شكل جديد من الإعلام، تعددت تصنيفاته ومسمياته لدى المهتمين والمختصين الإعلاميين، الذين أطلقوا عليه الإعلام الجديد، أو الإعلام البديل⁽¹⁾، الذي يشمل مواقع التواصل الاجتماعي.

(1) Jérôme Bossan: Le droit pénal confronté à la diversité des intermédiaires de l'internet, RSC, N° 02 du 16/08/2013, p.295 et s
Étienne Dreyfous & Jean Wahl: Questions-clés posées à l'Europe par les progrès des nouvelles technologies de l'information, Revue du Marché commun et de l'Union européenne, N° 416 du 10/03/1998,p161; Pascal Penaud: Nouvelles technologies de l'information: quel impact sur les organismes de Sécurité sociale, Droit social, N° 09-10 du 10/09/199, p769;

وتعد مواقع التواصل الاجتماعي من أحدث منتجات تقنية المعلومات والاتصالات وأكثرها شعبية، فهي تمتلك مجموعة من الخصائص التي تميزها عن المواقع الإلكترونية، مما جعلها الأكثر انتشاراً على شبكة الإنترنت، وهذا شجع متصفح شبكة الإنترنت من كافة أنحاء العالم على الإقبال المتزايد عليها.

ولقد ساعدت التطورات في تكنولوجيا الاتصال والإعلام على زيادة التواصل بين الأفراد على مستوى كافة المجتمعات بمختلف الثقافات والحضارات، متخطية كافة الحدود السياسية والثقافية، ومن ثم فقد أحدثت شبكة الإنترنت بتقنياتها وتطبيقاتها المتقدمة على الحاسب الآلي، والموبايل والتابلت درجة عالية من التأثير فاق ما أحدثته وسائل الاتصال والإعلام التقليدية⁽¹⁾، حيث يضم الإنترنت ملايين المواقع التي تتناول كافة المجالات السياسية والاقتصادية والاجتماعية، وغيرها، يجرى خلالها أشكال متنوعة من التواصل الاجتماعي، وأصبحت مواقع التعارف المعروفة

د/ مجدي محمد عبد الجواد الداغر، استخدامات الإعلاميين لشبكات التواصل الاجتماعي والإشباع المتحققة، دراسة تطبيقية على القائم بالاتصال بالمؤسسات الإعلامية بالسعودية، مجلة كلية الآداب، جامعة الزقازيق، العدد 64، مارس 2013، 534 وما بعدها؛ د/ زاهر راضي، استخدام مواقع التواصل الاجتماعي في العالم العربي، مجلة التربية، جامعة عمان الأهلية، 2003، ص23؛ د/ ياسر بكر، الإعلام البديل، مطابع حواس للنشر والتوزيع، القاهرة، 2010، ص34.

(1) Jacques Francillon: Messages racistes ou antisémites postés sur le réseau social Twitter, RSC, N° 03 du 20/11/2013, p.566 et s

بمواقع التواصل الاجتماعي⁽¹⁾ منها فيس بوك (facebook), تويتر (twitter), ماي سبيس (MySpace), وغيرها من مواقع التواصل الاجتماعي, والتطبيقات الداعمة

(1) تعتبر مواقع التواصل الاجتماعي إحدى أنواع المواقع الخدمية, حيث تتعدد المواقع الإلكترونية إلى عدة أنواع وهي:

المواقع الإلكترونية التي تقوم بمهام متعددة, وفقاً لغرض إنشائها, وتصنف هذه المواقع إلى أنماط متعددة تأخذ الصور التالية:

المواقع المعلوماتية:

وتضم هذه المواقع من حيث المحتوى والمضمون الذي يُنشر خلالها, منها:

المواقع التعريفية: تشمل مواقع الشركات والمؤسسات الشخصية وتتيح لزوارها الاطلاع على خدماتها ومنتجاتها ونشاطها, وهي بمثابة دليل تقدمه لزائريها وتقدم لهم معلومات بسيطة عما تريد الإعلان عنه , وعادة ما تذيّل المواضيع المنشورة فيها بعبارة "المزيد من التفاصيل زور الموقع التالي" , وتقوم تلك المواقع بالتعريف بأنشطة المؤسسات التي أسستها, مثل المؤسسات العلمية والفكرية والثقافية والخيرية.

المواقع المتخصصة: مواقع ذات أهمية لزوارها, لأنها تقدم المعرفة المتجددة والمعلومات في سياق تخصصي, تشمل شخصيات معينة أو مواضيع ذات أهمية أو مبتكرات علمية حديثة, ومن هذه المواقع, مواقع العلماء والشخصيات المشهورة وما يقدموه من جديد في مجالات العلم والمعرفة والثقافة والفنون, كالطب والعلوم الطبيعية, والمبتكرات الجديدة, والدورات الثقافية والمعرفية, وتقوم هذه المواقع على التعريف بالمشاهير في العلم من خلال المواقع الخاصة بذلك .

المواقع الإخبارية: تقدم أحدث آخر الأخبار من موقع الحدث وتهتم بالخبر الصحفي حين حدوثه وتجدد هذه المواقع وتحديث أخبارها في ضوء المستجدات التي تحدث في العالم, وهي عادةً ما تكون دعاية لبعض وسائل الإعلام المرئية والمكتوبة, كالمواقع الإلكترونية للفضائيات التليفزيونية مثل محطة (CNN, BBC ..إلخ), والصحف مثل الأهرام, اليوم السابع, المصري اليوم, الوفد...إلخ.

المنتديات: هي مواقع تتيح للأعضاء المنتسبين لها بالمشاركة في كتابة الموضوعات أو الرد على المواضيع التي يكتبها الآخرون, وهي مواقع منتشرة في الويب العربي.

المواقع الخدمية:

تقوم تلك المواقع على تقديم الخدمات المتنوعة لزوارها، ولا يقتصر على تقديم المعلومات العامة، ويُجرى تصنيفها على النحو التالي :

الشبكات الاجتماعية: تعتبر هذه الشبكات من أكثر المواقع على شبكة الإنترنت انتشاراً واستمراراً لتقديمها خاصية التواصل بين الأفراد والجماعات المستخدمين لها، حيث تمكنهم من التواصل وتبادل الأفكار والآراء والمعلومات والملفات والصور والفيديو، وهي مواقع انتشرت في السنوات الأخيرة بشكل كبير، وأصبحت أكبر وأضخم مواقع في فضاء الويب، ولا زالت مستمرة في الانتشار، وتقدم خدمة التواصل بين الأعضاء المنتسبين لها، حيث يمكن لأحد المستخدمين الارتباط بأحد الأصدقاء عبر الموقع ليصل الجديد مما يكتب ويضيف ذلك الصديق إلى الصفحة، كما أنها تمكن المستخدم من التحكم بالمحتوى الذي يظهر في صفحته، فلا يظهر إلا ما يضيفه الأصدقاء من الكتابات والصور ومقاطع الفيديو، من أشهر تلك المواقع فيس بوك، تويتر، يوتيوب .

خدمات مشاركة: هي مواقع متخصصة بنشر ومشاركة ملفات معرفية وعلمية وسياسية واجتماعية واقتصادية وثقافية ورياضية، وغيرها، من هذه المواقع اليوتيوب الذي يقدم الأحداث بالصور مثل (مقاطع الفيديو) وهي مواقع تتيح للآخرين وتنتشر ملفاتهم ومشاركة العالم المعرفة الموجودة في تلك الملفات، وتلك المواقع قد تكون متخصصة في نوع معين من الملفات مثل موقع اليوتيوب .

الخدمات البرمجية: تتميز هذه المواقع بتقديم خدمات خاصة ومهمة لمتصفحها على الإنترنت، فهي تقدم لهم برامج تساعد في القيام ببعض المهام، مثل تحرير الصور وتعديلها دون اللجوء لتصيب أو تحميل برامج أخرى، وتقوم بنفس الغرض على أجهزةهم الخاصة، وتغنيهم تلك المواقع عن البرامج التي تدور حول المهام المعقدة والتي تتطلب جهاز الكمبيوتر ذات مواصفات متنوعة ومتطورة، كما أنها توفر الجهد.

الخدمات السريعة: تتميز هذه المواقع بخدماتها البسيطة، لكنها في نفس الوقت تقدم خدمة ضرورية تتمثل في تقصير عناوين الصفحات الطويلة وجعلها قصيرة، يسهل إرسالها عبر موقع تويتر، وهذه الخدمة تتعلق بالمواقع الإلكترونية والشبكات الاجتماعية على وجه الخصوص، وهي مواقع تؤدي مهام بسيطة ولكنها مطلوبة، وعادة ما تكون هذه المهام متعلقة بمواقع إلكترونية أو

للاتصال مثل الواتس آب (WhatsApp), فايبر (Viber), سكاى بي (Skype) ,
إيمو (imo), وغيرها من أدوات التواصل, وتعتبر جميعها وسيلة للتواصل
الاجتماعي بين شعوب العالم, حيث ربطت تلك المواقع الأدوات مليارات الأشخاص
حول العالم, من خلال برامج رئيسة تتضمن محتوى ديناميكي يحتوي على
معلومات حول الشخصية, الاسم, والتاريخ الوظيفي, وغيره من البيانات الشخصية
والعائلية.

بشبكات اجتماعية أخرى, ويتميز هذا النوع عن السابق أن المهام تكون عادة بسيطة وسريعة في
نفس الوقت مطلوبة بين مستخدمي الإنترنت.

Étienne Dreyfous & Jean Wahl: Questions-clés posées à l'Europe par
les progrès des nouvelles technologies de l'information, Revue du
Marché commun et de l'Union européenne, N° 416 du
10/03/1998,p161; Pascal Penaud: Nouvelles technologies de
l'information : quel impact sur les organismes de Sécurité sociale, Droit
social, N° 09-10 du 10/09/199, p769;

د/ مجدي محمد عبد الجواد الداغر, استخدامات الإعلاميين لشبكات التواصل الاجتماعي
والإشباع المتحقق, دراسة تطبيقية على القائم بالاتصال بالمؤسسات الإعلامية بالسعودية,
مجلة كلية الآداب, جامعة الزقازيق, العدد 64, مارس 2013, 534 وما بعدها؛ د/ زاهر راضي,
استخدام مواقع التواصل الاجتماعي في العالم العربي, مجلة التربية, جامعة عمان الأهلية,
2003, ص23؛ د/ ياسر بكر, الإعلام البديل, مطابع حواس للنشر والتوزيع, القاهرة, 2010,
ص34.

ومواقع التواصل الاجتماعي كثيرة, بدأت في الظهور في عامي 2003، 2004 من
وقد نمت أعدادها بفضل مواقع (Facebook, MySpace, Skyrockblog)
وتتيح مواقع التواصل الاجتماعي للمستخدم إيجاد شخصية افتراضية تسمى الملف
الشخصي. ومواقع التواصل الاجتماعي حول العالم كثيرة وعديدة¹.

¹ أولاً: الفيس بوك facebook:

ثانياً: تويتر (twitter):

ثالثاً: يوتيوب (YouTube):

رابعاً: إنستجرام (Instagram):

خامساً: الكيك (keek):

سادساً: لينكد إن (LinkedIn):

الفرع الثالث

خصائص مواقع التواصل الاجتماعي

تعتبر مواقع التواصل الاجتماعي تقنية من التقنيات الحديثة في عالم التواصل بين الأفراد هي الأكثر انتشاراً على شبكة الإنترنت، لما تمتلكه من خصائص تميزها عن المواقع الإلكترونية مما شجع متصفح الإنترنت في كافة أنحاء العالم على الإقبال المتزايد.

تتسم مواقع التواصل الاجتماعي بمجموعة من المميزات والخصائص التي تميزها عن غيرها من المواقع الأخرى؛ حيث اكتسبت مواقع التواصل الاجتماعي هذه الخصائص والمميزات من السمات والمميزات الخاصة بتقنيات الجيل الثاني للويب عامة، وبسمات وخصائص مواقع التواصل الاجتماعي خاصة، فجعلت من المستخدم منتجاً للمحتوى ومعداً له، كما أتاحت له في الوقت نفسه المشاركة في المحتوى الذي أعده الآخرون، كما مكنت كل مستخدم من المساهمة بما يشاء من ملفات مصورة أو مكتوبة أو مبرمجة، وجعلت من صفحة كل مستخدم سبورة يكتب عليها ما يشاء، وما يكتبه على تلك الصفحة يشاهده الأصدقاء في الوقت نفسه، فعالم التواصل الاجتماعي غير كثيراً في أسلوب التواصل والمعرفة وطريقة عرضها، وجعل الفرد في اجتماع مستمر وهو في منزله.

أولاً: سهولة الاستخدام:

لا يحتاج التعامل مع مواقع التواصل الاجتماعي خبرة معلوماتية حتى يتم التفاعل مع محتواها، كما لا يحتاج رواد المواقع على خبرات وتدريبات علمية وعملية، وإنما إلى مجرد مقدمة ومبادئ أولية موجزة عن طبيعة الاستخدام، حيث تتطلب عملية التسجيل في مواقع التواصل الاجتماعي اختيار اسم ورقم سري، والموافقة على شروط العضوية، وبمجرد استكمال إجراءات التسجيل يحصل الفرد على عضوية باسم مستخدم ورقم سري، وحيز خاص به، يسمح له بمباشرة أعماله الرقمية بحرية تامة⁽¹⁾.

ثانياً: التفاعلية:

التفاعل هو قدرة وسيلة الاتصال الجديدة على الاستجابة لحديث المستخدم كما يحدث في عملية المحادثة بين شخصين، فالفرد فيها كما أنه مستقبل وقارئ، فهو مرسل وكاتب ومشارك⁽²⁾، فهي تلغي السلبية المقيتة في الإعلام القديم - التلفاز والصحف الورقية وتعطي حيزاً للمشاركة الفاعلة من المشاهد والقارئ.

(1) د/ مجدي محمد عبد الجواد الداغر، استخدامات الإعلاميين لشبكات التواصل الاجتماعي والإشباع المتحقق، دراسة تطبيقية على القائم بالاتصال بالمؤسسات الإعلامية بالسعودية، مجلة كلية الآداب، جامعة الزقازيق، العدد 64، مارس 2013، ص542.

p.252 et s. (2) Emilie Bailly & Emmanuel Daoud: op cit,

ثالثاً: إعلام متعدد الوسائط:

فلقد أحدثت ثورة نوعية في المحتوى الاتصالي الذي يتضمن على مزيج من النصوص والصور وملفات الصوت ومقاطع الفيديو, هذا المحتوى متعدد الوسائط, وانتشر بشكل كبير, وكانت لها تأثيرات اجتماعية وسياسية.

رابعاً: المجانية:

مواقع التواصل الاجتماعي اقتصادية في الجهد والوقت والمال, في ظل مجانية الاشتراك والتسجيل, فالفرد البسيط يستطيع امتلاك حيز على الشبكة للتواصل الاجتماعي, وليست ذلك حكراً على أصحاب الأموال, أو حكراً على جماعة دون أخرى.

خامساً: الحرية المطلقة:

جعلت مواقع التواصل الاجتماعي بإمكان أي شخص لديه الاتصال بشبكة الإنترنت أن يكون ناشراً وأن يوصل رسالته إلى جميع أنحاء العالم, وهناك العديد من الأخبار التي يمكن لمستخدميها مناقشة أي موضوع يخطر على بالهم مع عدد غير محدود من المستخدمين الآخرين في جميع أنحاء العالم, وقد أدى ذلك إلى رفع سقف حرية الرأي والتعبير والحصول على المعلومات.

سادساً: العالمية:

تلغى التواصل الاجتماعي الحواجز الجغرافية والمكانية، وتتخطى فيها الحدود الدولية، حيث يستطيع الفرد في الشرق التواصل مع الفرد في الغرب بكل بساطة وسهولة.

المطلب الثاني

أهمية مواقع التواصل الاجتماعي

تمهيد وتقسيم:

فرضت مواقع التواصل الاجتماعي نفسها وبقوة على المجتمعات، كما أحدثت ضجة كبيرة نتيجة ما قدمته من سهولة ويسر في التواصل بين الأفراد، واتسعت شهرتها وكثر استخدامها فأصبحت شغلهم الشاغل، حيث يتواصلون عبر هذه المواقع للتعارف ومعرفة أخبار الآخرين، وتلقي الأخبار والموضوعات وكل ما هو جديد في الساحة.

كما أنها تعمل على تقوية العلاقات بين أفراد المجتمع، وذلك من خلال مشاركة المعلومات بينهما، بالإضافة إلى تبادل الآراء والخبرات حول العديد من المواضيع، مما يؤدي إلى إكساب الأفراد الخبرة في العديد من المجالات.

وتبدو أهمية مواقع التواصل الاجتماعي في أنها تساعد مستخدميها على متابعة كل ما هو جديد في مجالات الحياة المتعددة، فهي توفر المعلومات التي تمنح مستخدميها فرصة التواصل لتبادل الأفكار والآراء، كما حولت المستخدم لها من متلق للمعلومات كما في وسائل الإعلام التقليدية إلى منتج للمعلومات ومشارك بها كما يشاء وبشكل حر للتعبير عن وجهات نظره.

لمواقع التواصل الاجتماعي أهمية كبيرة، فقد أصبحت شهرتها واسعة، وكثر التعامل معها بين جميع أفراد المجتمع؛ حيث يتواصلون عبر هذه المواقع للتعرف على

بعضهم ومعرفة أخبار بعضهم البعض، وإرسال رسائل وتلقي الأخبار والموضوعات وكل ما هو جديد في الساحة.

الفرع الأول: دور مواقع التواصل الاجتماعي في الإعلام.

الفرع الثاني: دور مواقع التواصل الاجتماعي في نشر الوعي السياسي والاجتماعي.

الفرع الثالث: دور مواقع التواصل الاجتماعي في التسويق الإلكتروني.

الفرع الرابع: دور مواقع التواصل الاجتماعي في جمع الاستدلالات.

الفرع الأول

دور مواقع التواصل الاجتماعي في الإعلام

من خلال تعريف مواقع التواصل وصورها يمكن استنتاج أهمية مواقع التواصل الاجتماعي في إتاحة المجال واسعًا أمام الإنسان للتعبير عن نفسه ومشاركة مشاعره وأفكاره مع الآخرين، خاصة وأن هناك حقيقة علمية وهي أن الإنسان اجتماعي بفطرته يتواصل مع الآخرين ولا يمكن أن يعيش في عزلة عن أخيه الإنسان، وقد أثبتت كثير من الدراسات والبحوث العلمية أن الإنسان لا يستطيع إشباع جميع حاجاته دون التواصل مع الآخرين، فحاجاته تفرض عليه العيش مع الآخرين لإشباع هذه الحاجات. أما الاحتياجات الاجتماعية فلا يمكن أن تقوم دون تواصل إنساني مع المحيط الاجتماعي، ولذلك فالإنسان كائن اجتماعي بطبيعته لا يمكن أن يعيش بمفرده.

باتت مواقع التواصل الاجتماعي وسيلة مؤثرة على الأحداث اليومية، وأتاحت الفرصة لجميع الأفراد لنقل أفكارهم ومناقشة قضاياهم الاجتماعية والاقتصادية والسياسية، وصارت مصدرا للصحفيين ووسائل الإعلام المختلفة والقنوات الفضائية التي باتت تنقل العديد من الأخبار والمعلومات، واستطاعت أن تفرض نفسها من

خلال المزايا والخدمات التي تقدمها هذه المواقع لمستخدميها من خلال مشاركة الأنشطة والاهتمامات⁽¹⁾.

فمواقع التواصل الاجتماعي تقدم معلومات كاملة وفورية حول القضايا المختلفة التي تهم المستخدمين، وتقوم على تسهيل متابعة ما ينشر من خلال الأفراد المستخدمين لهذه المواقع.

وأصبحت مصدر من مصادر الأخبار لكثير من روادها، وهي أخبار تتميز بأنها من مصدرها الأول وبصياغة فردية حرة غالباً، لا احترافية لاستخدامات مختلفة إعلامية أو اجتماعية.

فقد أدت التطورات الجديدة في تكنولوجيا الاتصال وثورة المعلومات إلى تغيير كبير في وسائل التواصل المستخدمة بين الإعلاميين، إذ بدأت الوسائل الإلكترونية تحتل مكانة مهمة في هذه المواقع، حتى أن الكثير من الخبراء والمتخصصين توقع أن تحل مواقع التواصل الاجتماعي محل الوسائل التقليدية المستخدمة في تحقيق التواصل فيما بينهم.

(1) José van Dijck & Thomas Poell: Understanding Social Media Logic, Media and Communication, Vol. 1, Issue 1, 13 Aug 2013 pp. 2-14; Gerald C. Kane & Maryam Alavi: What's Different About Social Media Networks? A Framework and Research Agenda, MIS Quarterly, Forthcoming, 25 Mar 2013, p.2 and others.

كما واكب ذلك تقدم هائل في الإمكانيات التي تتمتع بها تلك الوسائل والتي يمكن أن تعود بالفائدة على العمل الإعلامي، بما يجعلها وسائل اتصال مميزة وهي قائمة بذاتها، وتفوق في قدراتها وسائل التواصل التقليدية، فضلاً عن التقدم الكبير في نوعية وسائل التواصل الاجتماعي التي يمكن استخدامها في دعم التواصل بين الإعلاميين وتزايد عدد مستخدميها بشكل كبير على المستوى الوطني والدولي⁽¹⁾، قد انعكست هذه التطورات على المؤسسات الإعلامية التي لجأ بعضها للمواقع الإلكترونية للتواصل مع جمهورها كما انعكست على طبيعة المؤهلات اللازم توافرها في الإعلاميين على طبيعة الوسائل التي يستخدمونها في ممارسة عملهم الإعلامي، حيث أصبح لازماً عليهم إتقان التقنيات الحديثة في مجال التواصل مع المصادر الإعلامية للحصول على الأخبار والمعلومات⁽²⁾.

(1) د/ علي القرني، الإعلام الجديد، مكتبة الملك فهد للنشر، الرياض، 2011، ص22 إلى ص29.

(2) - د/ مجدي محمد عبد الجواد الداغر، مرجع السابق، ص527.

الفرع الثاني

دور مواقع التواصل الاجتماعي في نشر الوعي السياسي والاجتماعي

أحدثت مواقع التواصل الاجتماعي نقلة نوعية في الإعلام، استخدمت في البداية لأغراض التسلية والترفيه، ثم أصبحت إعلاماً محترفا ينقل المعلومات والأخبار للأفراد، فقد أصبح المشهد الإعلامي ملكا للجميع، ولم يعد مقتصرا على فئة محدودة من الأفراد، وأصبح المحتوى الإعلامي أكثر انتشارا وسرعة في الوصول إلى أكبر عدد من الأفراد، وبذلك أصبحت مواقع التواصل الاجتماعي أسهل وأقرب للأفراد.

وقد امتد التطور التقني إلى الحياة السياسية، ففي الوقت الذي تتدفق فيه المعلومات وتتسارع الأحداث بشكل تراكمي كبير، يجعل من الصعب التحكم فيها، احتلت مواقع التواصل الاجتماعي موقعا متميزا في سياق تحرير الفرد من مختلف أشكال التسلط والاستبداد السياسي، وتخلصه من الضغوط السياسية والاقتصادية والاجتماعية.

وأحدثت مواقع التواصل الاجتماعي تطورا كبيرا في تاريخ الإعلام، وأضحى الإعلام الجديد يؤثر في الحياة السياسية في المجتمعات، وجاءت لتشكّل عالماً افتراضيا يفتح المجال للأفراد والتجمعات والتنظيمات بمختلف أنواعها، لإبداء آرائهم

في القضايا والموضوعات التي تهمهم بحرية غير مسبوقه, وأصبح المواطن يصنع المحتوى الإعلامي ويناقش القضايا المختلفة بكل حرية⁽¹⁾.

واكتسبت مواقع التواصل الاجتماعي المزيد من الشعبية وازداد عدد مشتركها، لتصبح جزءاً من تاريخ التغيير السياسي والاجتماعي مقابل تراجع الإعلام التقليدي الرسمي، واستخدامها بشكل واضح في الحياة السياسية، فقد وفرت فرصاً عديدة للناشطين السياسيين وللمواطنين للتعبير عن آرائهم والتأثير في العملية السياسية وصنع القرار، فقد انتشر في المجتمعات استخدام هذه المواقع، ما ساهم في مشاركة سياسية فعالة ضد أنظمة فاسدة.

أدت مواقع التواصل الاجتماعي أدواراً مختلفة في الحياة السياسية، حيث ساهمت في خلق وعي تراكمي يقتضي التغيير لأنظمة.

كما لعبت مواقع التواصل الاجتماعي دوراً محورياً في انتخابات الولايات المتحدة الأمريكية عام 2016, وتعتبر هذه الانتخابات هي أول انتخابات "تويتر, فيس بوك" أو انتخابات إعلام اجتماعي رئاسي بامتياز⁽²⁾.

(1) Sarah Oates and Wendy W. Moe: Donald Trump and the 'Oxygen of Publicity': Branding, Social Media, and Mass Media in the 2016 Presidential Primary Elections, Paper prepared for the American Political Science Association Annual Meeting Political Communication Section, August 31, 2016,p.3.

(2) Sarah Oates and Wendy W. Moe: ibid,p.2.

الفرع الثالث

دور مواقع التواصل الاجتماعي في التسويق الإلكتروني

بعد ظهور التكنولوجيا الحديثة أصبح التواصل مع الآخرين أمراً سهلاً، فالعالم أصبح قرية صغيرة⁽¹⁾، وبعد ظهور مواقع التواصل الاجتماعي أصبح التواصل مباشراً، ولم يقتصر دور مواقع التواصل الاجتماعي على التواصل والإعلام ونشر الوعي، بل تعدى ليصبح أداة تسويقية للسلع والخدمات، والعقارات... إلخ، وذلك لما تملكه مواقع التواصل الاجتماعي من قوة التأثير لكونها إعلاماً فعالاً، وما زاد من فعاليتها كأداة للتجارة والتسويق، فمن خلالها يتم التواصل بين البائع والمشتري في أي وقت ومكان⁽²⁾.

(1) François-Guillaume Lassemlée-Léon & Aurélia Marie: La contrefaçon sur internet : nouvelles difficultés, nouveaux enjeux, AJ Pénal, N° 05 du 14/05/2012, p.263.

(2) Frank T. Piller & Alexander Vossen: From Social Media to Social Product Development: The Impact of Social Media on Co-Creation of Innovation, Die Unternehmung, Vol. 65, No. 1, 2012, p.2; Andrew T. Stephen & Jeff Galak: The Effects of Traditional and Social Earned Media on Sales: A Study of a Microlending Marketplace, Journal of Marketing Research, 49, 4 April 2012, p.1 and other.

حيث أدى توافر الأجهزة الحديثة والهواتف المحمولة والتطبيقات المتاحة عليها، مثل برنامج (olex) جعلت الفرد يحصل على أي سلعة أو عقار أو سيارة من أي مكان في العالم.

ولم يقتصر تأثير تقنيات التواصل الاجتماعي على الأفراد، بل على الاقتصاد أيضاً، حيث تقود الأعمال التجارية عبر مواقع التواصل إلى النمو الاقتصادي⁽¹⁾.

وتستخدم فرنسا مواقع التواصل في الأعمال التجارية، حيث تستخدمها بعض الشركات المدرجة في البورصة وأعضائها في الأعمال التجارية، حيث صدرت توصية صندوق النقد بالقرار رقم 15-2014 الصادر 9 ديسمبر 2014، وأوصت بأنه يمكن الاعتماد على مواقع التواصل الاجتماعي ومنها الفيس بوك (Facebook) وتويتر (Twitter) ولينكد ان (LinkedIn) لبث المعلومات الخاصة بالتوزيع أياً كانت الوسيلة المستخدمة، وذلك بشرط مطابقة المعلومات التي تنشرها للمعلومات التي أصدرتها الجهة الرئيسية، كما يجب أن تكون المعلومات التي

(1) Hailiang Chen&Prabuddha De: Wisdom of Crowds: The Value of Stock Opinions Transmitted Through Social Media, Review of Financial Studies (RFS), Forthcoming, 04 Oct 2016, p.3.

تصدرها دقيقة وصادقة، وقد لاقى استخدام مواقع التواصل الاجتماعي استجابة سريعة لدى نشطاء الأعمال التجارية⁽¹⁾.

ويخضع استخدام المواقع لقواعد الشفافية والمبادئ التوجيهية، فإن صندوق النقد العربي ينشر المعلومات على موقعه بحيث يكون من السهل الوصول إليها، مع مراعاة تحديثها باستمرار، ويتم حفظها لمدة لا تزيد على خمس سنوات، وإذا كانت الشركة لا تحتفظ بهذه الوثائق، توصي AMF أن يظهر موقعها الإلكتروني، حتى يمكن العثور على المعلومات القديمة عن طريق إدراج رابط معين إلى الموقع أرشيف الفرنسي. والواقع أن صندوق النقد العربي يذكر أنه بموجب التوجيه الشفافية، أنها ليست سوى وجود موقع التخزين الرئيسي الذي يتيح الحد من التزامات الأرشفة على مواقع ويب معين من الشركات المدرجة⁽²⁾.

يبدو لنا جلياً دور مواقع التواصل الاجتماعي في ترويج السلع والمنتجات بشكل سريع، حيث إنّ الإعلان من خلال هذه المواقع ينشر المنتج بشكل أسرع وأكبر

(1) Pierre-Henri Conac: Communication des sociétés cotées sur leur site internet et sur les médias sociaux, Revue des sociétés, N° 01 du 09/01/2015, p.62; Anne-Catherine Muller: Communications à destination des actionnaires individuels, Revue des sociétés, N° 01 du 08/01/2016, p.62.

(2) Pierre-Henri Conac: Communication des sociétés cotées sur leur site internet et sur les médias sociaux, op cit, p.62 et s.

للناس، أكثر ممّا يقدمه الإعلان التقليديّ في الصحف والمجلات، بالإضافة إلى توفير الوقت والجهد.

الفرع الرابع

دور مواقع التواصل الاجتماعي في جمع الاستدلالات

نتيجة لما تتميز به مواقع التواصل الاجتماعي من سهولة الحصول على المعلومات، فإنها تُعد حقلًا خصبًا للسلطات في الحصول على المعلومات، ويجوز استخدامها في جمع الاستدلالات في الجرائم.

وقد جاء القانون رقم 175 لسنة 2018، واعتد بالدليل الرقمي وعرفه: هو أية معلومات إلكترونية لها قوة أو قيمة ثبوتية مخزنة أو منقولة أو مستخرجة أو مأخوذة من أجهزة الحاسب أو الشبكات المعلوماتية وما في حكمها، والممكن تجميعه وتحليله باستخدام أجهزة أو برامج أو تطبيقات تكنولوجية خاصة⁽¹⁾.

أولاً: جمع الاستدلالات من مواقع التواصل الاجتماعي:

نصت المادة (11) من القانون رقم 175 لسنة 2018 على أن "يكون للأدلة المستمدة أو المستخرجة من الأجهزة أو المعدات أو الوسائط الدعائم الإلكترونية، أو النظام المعلوماتي أو من برامج الحاسب، أو من أي وسيلة لتقنية المعلومات نفس قيمة وحجية الأدلة الجنائية المادية في الإثبات الجنائي متى توافرت بها الشروط الفنية الواردة باللائحة التنفيذية".

(1) المادة الأولى من القانون رقم 175 لسنة 2018.

تُعتبر مواقع التواصل الاجتماعي أداة ممتازة لجمع المعلومات والأدلة الجنائية؛ لأنها تتضمن معلومات مهمة عن المستخدمين، وبالتالي يمكن للشرطة استخدامها في جمع الاستدلالات عن الجرائم، فهي تتميز بالتالي:

1- توفير الجهد والوقت والمال في جمع المعلومات، فمن خلالها يمكن التوصل إلى معلومات عن الهويتين الحقيقية والافتراضية. وتمثل هذه الوسائل فرصة حقيقية للسلطات في الوصول إلى المعلومات.

2- يمكن استخدام مواقع التواصل الاجتماعي في التحقيقات، وفي فرنسا تُستخدم أحد مواقع التواصل الاجتماعي الفيس بوك⁽¹⁾ لجمع المعلومات والاستدلالات في القضايا⁽²⁾، كجرائم الخطف، والتحريض على الانتحار أو الكراهية

(1) Laurence Usunier: La compétence des juridictions françaises pour connaître du différend entre le réseau social Facebook et l'un de ses membres, RTD Civ, N° 02 du 20/06/2016, p.310; Sophie André & Camille Lallemand: Facebook contre le consommateur français: l'hallali de la clause attributive, Dalloz IP/IT 2016 p.214; Cour d'appel de Paris, pôle 2, ch. 2, 12-02-2016, n° 15/08624, Cour de cassation, Chambre criminelle, 06-09-2016, n° 15-86.412.

(2) Jean-Pierre Gridel: Sophie Sontag-Koenig, Technologies de l'information et de la communication et défense pénale, RTD Civ, N° 04 du 19/12/2014, p.991; Pierre-Yves Verkindt: Nouvelles technologies de l'information et de la communication et nouvelles pratiques d'expertise Note de bas de page, Droit social, N° 01 du 10/01/2002, p.54.

العنصرية، والتشهير، والاتجار في الأعضاء البشرية، والمواد المخدرة، وجرائم الاعتراف الجنسي على الأطفال.

ولذلك يمكن استخدام هذه المواقع والصفحات الشخصية في إجراءات جمع الاستدلالات عن الجرائم بمعرفة الشرطة، فمن خلال تحليل مواقع الفيس بوك يمكن تحديد العلاقات بين المشتبه فيهم والجرائم الناشئة عن مواقع التواصل الاجتماعي. نعتقد أن المشرع المصري قد أحسن صنعا عندما نص في القانون رقم 175 لسنة 2018 على الاعتراف بالأدلة الإلكترونية التي لها قوة أو قيمة ثبوتية مخزنة أو منقولة أو مستخرجة أو مأخوذة من أجهزة الحاسب الآلي أو الشبكات المعلوماتية، وجعلها نفس قيمة وحجية الأدلة الجنائية المادية في الإثبات الجنائي مع توافر الشروط الفنية فيها؛ لكنه جانبه الصواب، حيث إنه أغفل ذكر أجهزة الهواتف المحمولة والتابلت.

ثانياً: شروط استخدام مواقع التواصل الاجتماعي في جمع الاستدلالات:

إذا كانت مواقع التواصل الاجتماعي توفر للسلطات معلومات مهمة عن مستخدمي هذه المواقع، فإنه ينبغي عند استخدام هذه المواقع في جمع الاستدلالات مراعاة الموازنة بين مصلحة الشخص في الحفاظ على سرية المعلومات والحق في الخصوصية من ناحية، ومصلحة العدالة في الوصول إلى المعلومات التي تسهم في كشف الحقيقة عن الجرائم المعلوماتية أو الجرائم الأخرى من ناحية أخرى، ويُشترط لاستخدام مواقع التواصل الاجتماعي في جمع الاستدلالات أن تتوفر الشروط التالية:

1- أن تقع الجريمة باستخدام مواقع التواصل الاجتماعي وتقنية المعلومات.

2- توافر الأدلة الكافية على وقوع الجريمة في حق الشخص المطلوب الحصول على بيانات عنه، أو البحث في الصفحة الشخصية الخاصة به على موقع التواصل الاجتماعي.

3- أن يقتصر على الحصول على المعلومات من الصفحة الشخصية دون البحث في الرسائل المخزنة آلياً لديه.

4- احترام الحق في الخصوصية، وضع الدستور المصري الصادر عام 2014 حدوداً لحماية الحق في الخصوصية، حيث نصت المادة (57) على أن "الحياة الخاصة حرمة، وهي مصونة لا تمس والمراسلات البريدية، والبرقية، والإلكترونية، والمحادثات الهاتفية، وغيرها من وسائل الاتصال حرمة، وسريتها مكفولة، ولا تجوز مصادرتها، أو الاطلاع عليها، أو رقابتها إلا بأمر قضائي مسبب، ولمدة محددة، وفي الأحوال التي بينها القانون". فإنه يجب الحصول على إذن من النيابة العامة، حيث إن المعلومات، والبيانات، والمستندات التي يتم تخزينها في ملفات تخص المستخدم أو على البريد الإلكتروني الخاص به تعد من الأسرار الخاصة التي لا يجوز انتهاكها إلا بإذن مسبب.

وفي هذا الصدد نصت المادة (6) من القانون رقم 175 لسنة 2018 على أن لجهة التحقيق المختصة، بحسب الأحوال أن تصدر أمراً مسبباً، لمأموري الضبط القضائي المختصين، لمدة لا تزيد على ثلاثين يوماً قابلة للتجديد لمرة واحدة، متى

كان لذلك فائدة في ظهور الحقيقة على ارتكاب جريمة معاقب عليها بمقتضى أحكام هذا القانون بواحد أو أكثر بما يأتي:

1- ضبط أو سحب أو جمع أو التحفظ على البيانات والمعلومات أو أنظمة المعلومات، وتتبعها في أي مكان أو نظام أو برنامج أو دعامة إلكترونية أو حاسب تكون موجودة فيه، ويتم تسليم أدلتها الرقمية للجهة مصدرة الأمر على ألا يؤثر ذلك على استمرارية النظم وتقديم الخدمة أن كان لها مقتضى.

2- البحث والتفتيش والدخول والنفوذ إلى برامج الحاسب وقواعد البيانات وغيرها من الأجهزة والنظم المعلوماتية تحقيقاً لغرض الضبط.

3- أن تأمر مقدم الخدمة بتسليم ما لديه من بيانات أو معلومات تتعلق بنظام معلوماتي أو جهاز تقني، موجودة تحت سيطرته أو مخزنة لديه، وكذا بيانات مستخدمي خدمته وحركة الاتصالات التي تمت على ذلك النظام أو الجهاز التقني. وفي كل الأحوال يجب أن يكون أمر جهة التحقيق المختصة مسبباً. ويكون استئناف الأوامر المتقدمة أمام المحكمة الجنائية المختصة منعقدة في غرفة المشورة في المواعيد، ووفقاً للإجراءات الجنائية".

ومن ثم فإنه يجوز الاعتداد والأخذ بالدليل المستمد من المعلومات التي تم الحصول عليها من مواقع التواصل الاجتماعي، وذلك مع مراعاة الشروط التي تجعل من ذلك الدليل مشروعاً؛ فعدم مشروعية الدليل من شأنه أن يهدر قيمته في الإثبات، ومن ثم لا يعول عليه كدليل في الإدانة.

وإزاء ذلك يجب تدريب مأموري الضبط بجرائم تقنية المعلومات فيما يتعلق بالأساليب الفنية المستخدمة في ارتكاب الجريمة، وفيما يتعلق بطرق الكشف عنها، والدلائل المستحدثة في مجال إثباتها وكيفية معاينتها، والتحفظ عليها، وكيفية فحصها فنياً، وذلك يتطلب تنمية استعدادهم وتكوين مهارات فنية، حتى يكون لديهم المعرفة الفنية تتناسب مع حجم المتغيرات والتطورات في مجال جرائم تقنية المعلومات.

ففي فرنسا تم صدور توصيات باستخدام مواقع التواصل الاجتماعي للهيئات القضائية، فقد نشرت كلية أخلاقيات القضاء الإداري في تقريرها السنوي للفترة من 1 أبريل 2018 إلى 31 مارس 2019، لمسألة استخدام الشبكات الاجتماعية من قبل أعضاء السلطة الإدارية، وتم دمج الممارسات الجيدة في المادة 47 من مدونة الأخلاقيات، وأوصى لهم بعدة توصيات منها عدم استخدام هذه الوسائط لغرض التعليق على الأخبار السياسية والاجتماعية وإظهار اليقظة في ملاحظاتهم على الأخبار القانونية والإدارية، كما تدعو مدونة الأخلاقيات المستخدمين إلى إعداد حساباتهم مسبقاً وإعدادها بشكل صحيح من أجل التحقق من إمكانية الوصول وضمان محدودية عدد جهات الاتصال وموثوقيتها⁽¹⁾.

(1)Emmanuelle Maupin: Recommandations sur l'utilisation des réseaux sociaux par les magistrats administratifs, AJDA, N° 15 du 22/04/2019 ,p. 840

وقد أقرت المادة (7) من القانون رقم 175 لسنة 2018 على الإجراءات والقرارات الصادرة بشأن حجب المواقع, حيث نصت على أن لجهة التحقيق المختصة، متى قامت أدلة على قيام موقع يبيث داخل الدولة أو خارجها، بوضع أي عبارات أو أرقام أو صور أو أفلام أو أية م مواد دعائية، أو ما في حكمها مما يعد جريمة من الجرائم المنصوص عليها بالقانون، وتشكل تهديدا للأمن القومي أو تعرض أمن البلاد أو اقتصادها القومي للخطر، أن تأمر بحجب الموقع أو المواقع محل البث، كلما أمكن تحقيق ذلك فنيا.

وعلى جهة التحقيق عرض أمر الحجب على المحكمة المختصة منعقدة في غرفة المشورة، خلال أربع وعشرين ساعة، مشفوعا بمذكرة برأيها، وتصدر المحكمة قرارها في الأمر مسببا، في مدة لا تتجاوز اثنين وسبعين ساعة من وقت عرضه عليها، بالقبول أو بالرفض.

ويجوز في حالة الاستعجال لوجود خطر حالاً أو ضرر وشيك الوقوع من ارتكاب جريمة، أن تقوم جهات التحري والضبط المختصة بإبلاغ الجهاز ليقوم بإخطار مقدم الخدمة على الفور بالحجب المؤقت للموقع أو المواقع أو الروابط أو المحتوى المذكور في الفقرة الأولى من هذه المادة وفقا لأحكامها. ويلتزم مقدم الخدمة بتنفيذ مضمون الإخطار فور وروده إليه.

وعلى جهة التحري والضبط المبلغة أن تعرض محضرا تثبت فيه ما تم من إجراءات على جهة التحقيق المختصة، وذلك خلال ثمانٍ وأربعين ساعة من تاريخ الإبلاغ الذي وجهته للجهاز، وتتبع في هذا المحضر ذات الإجراءات المبينة بالفقرة

الثانية من هذه المادة، وتصدر المحكمة المختصة قرارها في هذه الحالة، أما بتأييد ما تم من إجراءات حجب أو بوقفها. فإذا لم يعرض المحضر المشار إليه في الفقرة السابقة في الموعد المحدد، يعد الحجب الذي تم كأن لم يكن.

المبحث الثاني

نطاق المسؤولية الجنائية لإساءة استخدام مواقع التواصل الاجتماعي

تمهيد وتقسيم:

إذا كانت مواقع التواصل الاجتماعي توفر مميزات للمستخدمين بالتواصل وتبادل المعلومات عبر شبكة الإنترنت، ففي المقابل تُعد مسرحاً خصباً لجرائم النشر الإلكتروني، الأمر الذي يُثير العديد من المشكلات.

فهناك العديد من الظواهر السلبية في مواقع التواصل الاجتماعي ومدى إمكانية مساءلة أصحابها جنائياً، مثل ما يقع من الاعتداء على النظام العام فيه⁽¹⁾، وكذلك ما يكون في هذه الوسائل من النشر الإباحي بنشر الصور والمقاطع الجنسية، وكذلك ما يقع على الأفراد من إساءات كالسب والتشهير خصوصاً عند الاختلاف في المجال الفكري والسياسي، وما يحدث بين الإعلاميين من إساءات.

وإذا كانت حرية الرأي والتعبير من الحريات والحقوق المعترف بها دولياً وداخلياً، وسواء أكان ذلك في الإعلام التقليدي أم الإعلام الجديد، فإن ممارستها أو إساءة استعمالها، وإطلاق العنان لها من شأنه أن يؤدي إلى المساس بحقوق آخرين وحررياتهم أو أن يلحق الأذى المعنوي أو المادي بهم؛ خاصة في ظل الانتشار الكبير لمواقع التواصل الاجتماعي، التي تبث مادتها من خلال شبكة الإنترنت

(1) Nicolas Verly: Diffamations et injures publiques sur les réseaux sociaux : définitions, responsabilités et sanctions, AJ Collectivités Territoriales, N° 12 du 16/12/2014, p.589 et s.

والتي أصبحت مجال لبعض ضعاف النفوس للتشهير بالناس ومس سمعتهم والتدخل في خصوصياتهم؛ أو للإشادة بالعنف أو التحريض على الكراهية أو العنصرية والإرهاب، أو المساس بالنظام العام أو الأمن والدفاع الوطنيين في الدولة، من خلال إنشاء مواقع إلكترونية تحض على ارتكاب جرائم ضد أمنها وسلامتها الإقليمية واستقرارها، وضد نظام الحكم في الدولة.

حيث إن الجرائم عبر مواقع التواصل الاجتماعي ليست ذات صورة واحدة، وإنما تأخذ أشكالاً وصوراً متعددة⁽¹⁾، قد تكون جرائم أموال، كجرائم النصب، والاحتيال الإلكتروني والاعتداء على بطاقات البنوك والخدمات وأدوات الدفع الإلكتروني، وقد تكون جرائم ضد الأشخاص ومن ذلك جرائم السب والقذف والتشهير والابتزاز، والاعتداء على حرمة الحياة الخاصة، وقد تكون جرائم ماسة بأمن الدولة كجرائم الإرهاب الإلكتروني.

وإذا كان البحث يقتصر على الحماية الجنائية من إساءة استخدام مواقع التواصل الاجتماعي، في هذا الصدد نلقي الضوء على أهم الجرائم التي تنجم عن إساءة استخدام هذه المواقع على النحو التالي.

المطب الأول: جرائم الأشخاص عبر مواقع التواصل الاجتماعي.

المطب الثاني: جرائم الأموال عبر مواقع التواصل الاجتماعي.

(¹) Delphine Castel: Réseaux sociaux – Comment Internet transforme la politique pénale, JA , N° 600 du 01/06/2019, p.9

المطب الثالث: الإرهاب عبر مواقع التواصل الاجتماعي.

المطلب الأول

جرائم الأشخاص عبر مواقع التواصل الاجتماعي

تمهيد وتقسيم:

كثرت في الحقبة الأخيرة مواقع التواصل الاجتماعي وتعددت استخداماتها ومميزاتها؛ لكن للأسف الشديد تحولت مواقع التواصل الاجتماعي من النعمة إلى نقمة بسبب سوء الاستخدام من قبل بعض الأفراد الذين تسببوا في إزعاج وقلق الغير، وهؤلاء العابثون نتيجة تصرفاتهم السيئة جلبوا لغيرهم أضرار، ذهب ضحيتها كثير من الأبرياء وأصبحت تداهمهم مشاكل عديدة.

وسوف نتناول في هذا المطلب تجريم المساس بالأشخاص عبر مواقع التواصل الاجتماعي على النحو التالي:

الفرع الأول: السب والقذف عبر مواقع التواصل الاجتماعي.

الفرع الثاني: جريمة الدخول غير المصرح عبر مواقع التواصل الاجتماعي.

الفرع الثالث: جرائم النشر الإلكتروني عبر مواقع التواصل الاجتماعي.

الفرع الرابع: المسؤولية الجنائية لمقدمي الخدمات الإلكترونية عبر مواقع التواصل الاجتماعي.

الفرع الأول

القذف والسب عبر مواقع التواصل الاجتماعي

تعد جرائم السب والقذف من الجرائم التي لها الأثر البالغ على الإنسان، وهي الأكثر شيوعاً وانتشاراً خاصة عبر مواقع التواصل الاجتماعي، إذ يساء استخدامها للنيل من شرف وكرامة الغير أو تعرضه إلى بغض الناس واحتقارهم.

قد يلجأ الكثير من رواد مواقع التواصل الاجتماعي فيس بوك وغيرها إلى توجيه عبارات وألفاظ عن طريق الأنترنت مما يصيب الأشخاص بأضرار جسيمة، وذلك عن طريق وضع مشاركات على المنشورات يتضمن عبارات سب وقذف يمكن لأي زائر مشاهدتها، لذا كان لابد من إلقاء الضوء على مثل هذه الأفعال.

النص القانوني:

لم ينص المشرع المصري في القانون رقم 175 لسنة 2018 على تجريم السب والقذف عبر مواقع التواصل الاجتماعي، على خلاف القوانين المقارنة الأخرى.

ففي القانون الإماراتي نصت المادة (20) من المرسوم الإماراتي رقم (5) لسنة 2012 على أن "مع عدم الإخلال بأحكام جريمة القذف المقررة في الشريعة الإسلامية، يعاقب بالحبس والغرامة التي لا تقل عن مائتين وخمسين ألف درهم ولا تتجاوز خمسمائة ألف درهم أو بإحدى هاتين العقوبتين كل من سب الغير أو أسند إليه واقعة من شأنها أن تجعله محلاً للعقاب أو الازدراء من قبل الآخرين، وذلك

باستخدام شبكة معلوماتية، أو وسيلة تقنية معلومات. فإذا وقع السب أو القذف في حق موظف عام أو مكلف بخدمة عامة بمناسبة أو بسبب تأدية عمله عد ذلك ظرفاً مشدداً للجريمة".

ونص القانون العماني رقم (12) لسنة 2011 أيضاً على تجريم السب والقذف باستخدام شبكة المعلومات ومنها مواقع التواصل الاجتماعي، حيث نصت المادة (16) على أن يعاقب بالسجن مدة لا تقل عن سنة ولا تزيد على ثلاث سنوات وبغرامة لا تقل عن ألف ريال عماني ولا تزيد على خمسة آلاف ريال عماني أو بإحدى هاتين العقوبتين، كل من استخدم الشبكة المعلوماتية أو وسائل تقنية المعلومات كالهواتف النقالة المزودة بآلة تصوير في الاعتداء على حرمة الحياة الخاصة أو العائلية للأفراد وذلك بالتقاط صور أو نشر أخبار أو تسجيلات صوتية أو مرئية تتصل بها ولو كانت صحيحة، أو في التعدي على الغير بالسب أو القذف.

أولاً: القذف عبر مواقع التواصل الاجتماعي:

عرف قانون العقوبات القذف بأنه إسناد واقعة محددة تستوجب عقاب من تُنسب إليه أو احتقاره عند أهله ووطنه.

ويمكننا تعريف القذف عبر مواقع التواصل الاجتماعي بأنه إسناد شخص واقعة معينة على إحدى صفحات التواصل الاجتماعي مما تستلزم عقاب من تنسب إليه أو احتقار الأعضاء أو المجتمع له.

أركان جريمة القذف عبر مواقع التواصل الاجتماعي:

الركن المادي:

يتحقق الركن المادي بتوافر ثلاثة عناصر.

فعل الإسناد: نسبة واقعة معينة إلى شخص على إحدى صفحات مواقع التواصل الاجتماعي.

موضوع الإسناد: أن ينصب الإسناد على واقعة ماسة بالشرف والاعتبار, ويجب أن تكون مستوجبة العقاب أو الاحتقار لمن أُسندت إليه.

علانية الإسناد: اتصال علم الجمهور بالتعبير الصادر من المتهم أو رأيه أو شعوره عبر مواقع التواصل الاجتماعي, بنشر مقاطع فيديو أو صوت أو صور أو بالكتابة.

الركن المعنوي:

يعد القذف في جميع حالاته جريمة عمدية, لا بد من توافر القصد الجنائي, وهي أن تتجه إرادة القاذف عبر مواقع التواصل الاجتماعي إلى إذاعة الأمور المتضمنة القذف, مع علمه بانها لو كانت صادقة لأوجبت مسؤولية الشخص المقذوف أو احتقاره.

العقوبة:

لم ينص المشرع المصري في القانون رقم 175 لسنة 2018 على تجريم السب والكذب عبر مواقع التواصل الاجتماعي، إنما نص على تجريم الكذب⁽¹⁾ والسب وفقاً للقواعد العامة⁽²⁾، إلا أن التشريعات الأخرى⁽¹⁾ تدخلت بتجريم ذلك.

⁽¹⁾ نصت المادة (303) من قانون العقوبات على أن يعاقب على الكذب بغرامة لا تقل عن سبعة آلاف وخمسمائة جنيه ولا تزيد على اثنين وعشرين ألف وخمسمائة جنيه. فإذا وقع الكذب في حق موظف عام أو شخص ذي صفة نيابية عامة أو مكلف بخدمة عامة، وكان ذلك بسبب أداء الوظيفة أو النيابة أو الخدمة العامة، كانت العقوبة الغرامة التي لا تقل عن خمسة عشر ألف جنيه ولا تزيد عن ثلاثين ألف جنيه.

⁽²⁾ جرمت القواعد العامة السب، حيث نصت المادة (306) من قانون العقوبات والتي على أن "كل سب لا يشتمل على إسناد واقعة معينة بل يتضمن بأي وجه من الوجوه خدشاً للشرف أو الاعتبار يعاقب عليه في الأحوال المبينة بالمادة 171 بغرامة لا تقل عن ألفي جنيه ولا تزيد على عشرة آلاف جنيه."

- كما أنه من المقرر بنص المادة 308 أن "إذا تضمن العيب أو الإهانة أو الكذب أو السب الذي ارتكب بإحدى الطرق المبينة في المادة (171) طعنًا في عرض الأفراد أو خدشاً لسمعة العائلات تكون العقوبة الحبس والغرامة معاً في الحدود المبينة في المواد 179 و181 و182 و303 و306 و307 على ألا تقل الغرامة في حالة النشر في إحدى الجرائد أو المطبوعات عن نصف الحد الأقصى وألا يقل الحبس عن ستة شهور."

- كما أنه من المقرر بنص المادة 308 مكرر أن "كل من كذب بغيره بطريق التليفون يعاقب بالعقوبات المنصوص عليها في المادة 303. وكل من وجه إلى غيره بالطريق المشار إليه بالفقرة السابقة سباً لا يشتمل على إسناد واقعة معينة بل يتضمن بأي وجه من الوجوه خدشاً للشرف أو الاعتبار يعاقب بالعقوبة المنصوص عليها في المادة 306. وإذا تضمن العيب أو الكذب أو السب الذي ارتكب بالطريق المبين بالفقرتين السابقتين طعنًا في عرض الأفراد أو خدشاً لسمعة العائلات يعاقب بالعقوبة المنصوص عليها في المادة 308."

وقد عاقبت (20) من المرسوم الإماراتي رقم (5) لسنة 2012 بالحبس والغرامة التي لا تقل عن مائتين وخمسين ألف درهم ولا تجاوز خمسمائة ألف درهم أو بإحدى هاتين العقوبتين كل من سب الغير أو أسند إليه واقعة من شأنها أن تجعله محلاً للعقاب أو الازدراء من قبل الآخرين، وذلك باستخدام شبكة معلوماتية، أو وسيلة تقنية معلومات. فإذا وقع السب أو القذف في حق موظف عام أو مُكلف بخدمة عامة بمناسبة أو بسبب تأدية عمله عد ذلك ظرفاً مشدداً للجريمة.

والقانون العماني رقم (12) لسنة 2011 عاقب أيضاً في المادة (16) بالحبس مدة لا تقل عن سنة ولا تزيد على ثلاث سنوات وبغرامة لا تقل عن ألف ريال عماني ولا تزيد على خمسة آلاف ريال عماني أو بإحدى هاتين العقوبتين، كل من

حيث إنه من المقرر بنص المادة 70 من قانون تنظيم الاتصالات رقم 10 لسنة 2003 أن "مع عدم الإخلال بأية عقوبة أشد منصوص عليها في قانون العقوبات أو في أي قانون آخر يعاقب على الجرائم المنصوص عليها في المواد التالية بالعقوبات المقررة فيها".

- كما أنه من المقرر بنص المادة 2/76 من ذات القانون أن "مع عدم الإخلال بالحق في التعويض المناسب، يعاقب بالحبس وبغرامة لا تقل عن خمسمائة جنيه ولا تجاوز عشرين ألف جنيه أو بإحدى هاتين العقوبتين كل من: ... 2- تعمد إزعاج أو مضايقة غيره بإساءة استعمال أجهزة الاتصالات".

(1) نصت المادة الثالثة من القانون السعودي على أن "يعاقب بالسجن مدة لا تزيد عن سنة وبغرامة لا تزيد على خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أيًا من الجرائم المعلوماتية الآتية:

1-...-2؛...-3؛...-4؛...-5-التشهير بالآخرين، وإلحاق الضرر بهم، عبر وسائل تقنيات المعلومات المختلفة".

استخدم الشبكة المعلوماتية أو وسائل تقنية المعلومات كالهواتف النقالة المزودة بآلة تصوير في التعدي على الغير بالسب أو القذف.

ثانياً: السب عبر مواقع التواصل الاجتماعي:

عرف السب بأنه إسناد واقعة غير معينة لشخص خادشة لشرفه واعتباره.

ويمكننا تعريف السب عبر مواقع التواصل الاجتماعي بأنه إسناد شخص واقعة غير معينة على إحدى صفحات مواقع التواصل الاجتماعي خادشة لشرفه واعتباره.

الركن المادي:

صور السب عبر مواقع التواصل الاجتماعي:

السب القولي: كل اعتداء بالقول على الآخرين عن طريق التسجيل الصوتي أو عبر مقاطع الفيديو أو اليوتيوب أو الكيك, وغيره.

السب الكتابي: كل اعتداء على الآخرين عن طريق الكتابة على الفيس بوك أو تويتر, أو نشر صور أو إعادة نشر صور ساخرة للآخرين.

فمواقع التواصل الاجتماعي كالفيس بوك وتويتر, وغيرها, تتميز بالحرية وغياب الرقابة, مليئة بأنواع السب والشتم.

يتمثل الركن المادي في خدش الشرف والاعتبار بأي شكل من الأشكال موجه ضد شخص معين دون إسناد واقعة معينة, وذلك بصورة علنية, ونظراً لاتفاق السب مع القذف في عنصر العلنية فإننا نحيل إلى ما سبق ذكره منعاً للتكرار.

الركن المعنوي:

يتوافر علم الجاني بمعنى الأمور المتضمنة للسب الذي نشره على صفحة موقع التواصل الاجتماعي, وذلك العلم يكون مفترضاً متى كانت عبارات السب شائنة وجارحة, وأن يتوافر لدى الجاني قصد الإذاعة والإعلان, وأن تكون إرادته اتجهت إلى نشر ما عبر عنه من معنى يخذش شرف واعتبار المجني عليه.

العقوبة:

لم ينص المشرع المصري في القانون رقم 175 لسنة 2018 على تجريم السب والقذف عبر مواقع التواصل الاجتماعي, إنما نص على تجريم السب وفقاً للقواعد العامة, إلا أن التشريعات الأخرى تدخلت بتجريم ذلك, نصت المادة (20) من المرسوم الإماراتي رقم (5) لسنة 2012 على أن "مع عدم الإخلال بأحكام جريمة القذف المقررة في الشريعة الإسلامية, يعاقب بالحبس والغرامة التي لا تقل عن مائتين وخمسين ألف درهم ولا تتجاوز خمسمائة ألف درهم أو بإحدى هاتين العقوبتين كل من سب الغير أو أسند إليه واقعة من شأنها أن تجعله محلاً للعقاب أو الازدراء من قبل الآخرين, وذلك باستخدام شبكة معلوماتية, أو وسيلة تقنية معلومات. فإذا وقع السب أو القذف في حق موظف عام أو مُكلف بخدمة عامة بمناسبة أو بسبب تأدية عمله عد ذلك ظرفاً مشدداً للجريمة".

ونص القانون العماني كذلك على تجريم السب عبر المواقع الإلكترونية⁽¹⁾, ومنها مواقع التواصل الاجتماعي.

وقد ذهب اتجاه في الفقه الفرنسي⁽²⁾ إلى اعتبار استخدام مواقع التواصل الاجتماعي في السب بمثابة انتهاك لحرية الرأي والتعبير, وكذلك الأحكام القضائية⁽³⁾.

ثالثاً: التشهير عبر مواقع التواصل الاجتماعي:

يقصد به نشر أو نقل وقائع أو بيانات فيها معنى الإساءة أو الإهانة لشخص مما يترتب عليها الحط من كرامته أو سمعته أو شرفه, غالباً ما يحدث في الواقع العملي, خاصة في مواقع التواصل الاجتماعي تنشر وقائع تنال من كرامة الأشخاص من سب وقذف وتطاول بلا وازع من ضمير وبلا حساب.

وفي هذا الصدد نص القانون رقم 175 لسنة 2018 في المادة (26) على أن "يعاقب بالحبس مدة لا تقل عن سنتين ولا تجاوز خمس سنوات وبغرامة لا تقل عن مائة ألف جنيه لا تجاوز ثلاثمائة ألف جنيه أو بإحدى العقوبتين كل من تعمد استعمال برنامج معلوماتي أو تقنية معلوماتية في معالجة معطيات شخصية للغير

(1) المادة (16) من القانون رقم (12) لسنة 2011.

(2) Nicolas Verly: Diffamations et injures publiques sur les réseaux sociaux: définitions, responsabilités et sanctions, AJ Collectivités Territoriales, N° 12 du 16/12/2014, p.589.

(3) Cour de cassation, Chambre criminelle, 02-11-2016, n° 15-87.163; Cour de cassation, Chambre criminelle, 7 février 2017, N° 15-83439.

لربطها بمحتوى مناف للأداب العامة أو لإظهارها بطريقة من شأنها المساس باعتباره أو شرفه".

وقد عاقب المشرع الإماراتي التشهير باستخدام الوسائل الإلكترونية، نصت المادة (21) من القانون على أن "...كما يعاقب بالحبس مدة لا تقل عن سنة واحدة والغرامة التي لا تقل عن مائتين وخمسون ألف ولا تجاوز خمسمائة ألف درهم أو بإحدى هاتين العقوبتين كل من استخدم نظام معلومات إلكترونية أو إحدى وسائل تقنية المعلومات، لإجراء أي تعديل أو معالجة على تسجيل أو صورة أو مشهد، بقصد التشهير أو الإساءة إلى شخص آخر، أو الاعتداء على خصوصيته أو انتهاكها".

نعتقد أن لجوء بعض الأشخاص إلى هذه النوعية من الجرائم يرجع إلى اعتقادهم بصعوبة اكتشافهم والإفلات من العقوبة، في حين أن الجريمة المعلوماتية تخضع في وسائل إثباتها إلى طرق أخرى بخلاف الجريمة التقليدية إذ إن وجود الجريمة الإلكترونية يتطلب وجود بيئة رقمية واتصال بالإنترنت، وبالتالي فإن إثباتها يتطلب استخدام أجهزة تقنية عالية لمعرفة طريقة حدوث وكيفية ارتكاب الجريمة ونسبتها إلى الشخص الذي قام بالتعدي على حقوق الآخرين بإحدى الطرق.

حيث إن هذا النوع من الجرائم يصعب في بعض الحالات اكتشافها أو العجز عن إثباتها كونها جريمة متعدية الحدود وتتم في أكثر من دولة، ولكنها بالمقابل متى

ثبت ارتكاب الجاني للجريمة عن طريق عنوان جهاز الاتصال أو الأدلة والقرائن المرتبطة بها، ففي هذه الحالة يصعب الإفلات من العقوبة.

فإن من يرتكب جريمة السب والقذف والتشهير عبر مواقع التواصل الاجتماعي غالباً ما يفتقد للوزع الديني والأخلاقي، هذا بالإضافة إلى التقدم التقني ساعد في تسهيل الأمور الحياتية في العصر الحديث، ومن الطبيعي أن تكون هناك بعض المخاطر المتعلقة بإساءة استخدام مواقع التواصل الاجتماعي، مما يتعين وجود قانون في مصر لمكافحة ومعاقبة مرتكبي الجرائم المعلوماتية، ففي تقرير تلك المسئولية يعد بمثابة حماية للحق في الخصوصية تبدأ من الشخص نفسه، من خلال معرفة طبيعة الجريمة المعلوماتية وعقوبتها، وزيادة الوعي بمخاطر التقنية وأهمية حماية مواقع التواصل الاجتماعي والمعلومات والأجهزة والبرامج من الاعتداء عليها بالاختراق.

رابعاً: الاعتداء على حرمة الحياة الخاصة:

نص القانون المصري رقم 17 لسنة 2018 على تجريم الاعتداء على حرمة الحياة الخاصة، وذلك ما أكدته المادة (25) من القانون على أن يعاقب بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من اعتدى على أي من المبادئ أو القيم الأسرية في المجتمع المصري، أو انتهك حرمة الحياة الخاصة أو ارسل بكثافة العديد من الرسائل الإلكترونية لشخص معين دون موافقته، أو منح بيانات إلى

نظام أو موقع الكترونى لترويج السلع أو الخدمات دون موافقته أو بالقيام بالنشر عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات، لمعلومات أو أخبار أو صور وما في حكمها، تنتهك خصوصية أي شخص دون رضاه، سواء كانت المعلومات المنشورة صحيحة أم غير صحيحة.

ونصت المادة (26) من القانون على أن يعاقب بالحبس مدة لا تقل عن سنتين ولا تجاوز خمس سنوات وبغرامة لا تقل عن مائة ألف جنيه لا تجاوز ثلاثمائة ألف جنيه أو بإحدى العقوبتين كل من تعمد استعمال برنامج معلوماتي أو تقنية معلوماتية في معالجة معطيات شخصية للغير لربطها بمحتوى مناف للأداب العامة أو لإظهارها بطريقة من شأنها المساس باعتباره أو شرفه.

وبذلك يكون القانون رقم 175 لسنة 2018 تصدى لجرائم الفوتوشوب الخاصة بتعديل وتركيب الصور، حيث ازدادت تلك الجرائم بشكل خطير، وتعرض المجتمع لأخطار فادحة من أفراد تخصصت في فعل ذلك، مستغلين الإنترنت، وخاصة مواقع التواصل الاجتماعي، فقد أحسن المشرع المصري صنعاً لمواجهة كل هذه الأخطار الإجرامية.

الفرع الثاني

جريمة الدخول غير المصرح على مواقع التواصل الاجتماعي

يعد الدخول غير المشروع إلى أنظمة الحاسب الآلي من أخطر الجرائم التي تهدد تقنية المعلومات، لا سيما أن العديد من تلك الأنظمة تمتلكها الحكومات وتحتوي على العديد من المعلومات ذات أهمية للدولة، ويشكل اعتداء على خصوصية الأفراد.

وقد يستغل الفيس بوك (Facebook) في التعرف إلى بيانات الأشخاص من خلال معلوماتهم وجهات الاتصال الخاصة بهم، وعناوين البريد الإلكتروني، ومعرفة كلمة السر، ثم الدخول إلى صفحاتهم الشخصية.

النص القانوني:

لم ينص المشرع المصري على تجريم الدخول غير المشروع لمواقع التواصل الاجتماعي صراحة إلا أنه نص في القانون رقم 175 لسنة 2018 على أن يعاقب بالحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو إحدى هاتين العقوبتين، كل من دخل عمداً أو دخل بخطأ غير عمدى وبقي بدون وجه حق، على موقع أو حساب خاص أو نظام معلوماتي محظور الدخول عليه.

فإذا أنتج عن ذلك إتلاف أو محو أو تغيير أو نسخ أو إعادة نشر للبيانات أو المعلومات الموجودة على ذلك الموقع أو الحساب الخاص أو النظام المعلوماتي،

تكون العقوبة الحبس مدة لا تقل عن سنتين وبغرامة لا تقل عن 100 ألف جنيه ولا تجاوز 200 ألف أو بإحدى هاتين العقوبتين. حيث جرم المشرع المصري دخول موقعاً أو نظاماً معلوماتياً عمدي أو غير عمدي، وشدد العقوبة في حالة حدوث إتلاف أو محو أو تغيير أو نسخ أو إعادة نشر للبيانات أو المعلومات الموجودة على ذلك الموقع أو الحساب الخاص أو النظام المعلوماتي.

هذا بالإضافة إلى تجريم تجاوز حدود الحق في الدخول، فقد جاء نص المادة (15) من القانون على أن يعاقب بالحبس مدة لا تقل عن 6 أشهر وبغرامة لا تقل عن ثلاثين ألف جنيه ولا تجاوز خمسين ألف جنيه، أو بإحدى هاتين العقوبتين، كل من دخل إلى موقع أو حساب خاص أو نظام معلوماتي مستخدماً حقاً مخولاً له، فتعدى حدود هذا الحق من حيث الزمان أو مستوى الدخول.

جرمت غالبية القوانين والتشريعات المقارنة الدخول غير المشروع إلى أنظمة الحاسب الآلي، نص المشرع الفرنسي في المادة (323-1) من قانون العقوبات على أن يُعاقب كل من دخل أو بقي عن طريق الاحتيال، في نظام المعالجة الآلية للبيانات أو المعلومات أو جزءاً منها بالحبس سنتين (القانون رقم 912-2015 الصادر 24 يوليو 2015)⁽¹⁾ وغرامة قدرها 60 ألف يورو. وإذا ترتب على ذلك

(1) JORF n°0171 du 26 juillet 2015 page 12735, texte n° 2, LOI n° 2015-912 du 24 juillet 2015 relative au renseignement.

حذف البيانات الواردة في النظام أو تعديلها، أو تعطيل أداء هذا النظام، فإن العقوبة تكون السجن ثلاث سنوات وغرامة قدرها 100 ألف يورو.

(القانون رقم 410-2012 الصادر 27 مارس 2012)⁽¹⁾ وتشدد العقوبة لتصبح السجن لمدة خمس سنوات وغرامة قدرها 150 ألف يورو، وذلك في حالة ارتكاب الجرائم الواردة في الفقرتين ضد نظام المعالجة الآلية للبيانات الشخصية المحفوظة على أجهزة الدولة⁽²⁾.

(1) JORF n°0075 du 28 mars 2012 page 5604, texte n° 2, LOI n° 2012-410 du 27 mars 2012 relative à la protection de l'identité.

(2) Art. 323-1 "Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de (L. n° 2004-575 du 21 juin 2004, art. 45-I) «deux ans» d'emprisonnement et de (L. n° 2015-912 du 24 juill. 2015, art. 4) «60 000 €» d'amende.

Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de (L. no 2004-575 du 21 juin 2004, art. 45-I) «trois ans» d'emprisonnement et de (L. n° 2015-912 du 24 juill. 2015, art. 4) «100 000 €» d'amende.

(L. n° 2012-410 du 27 mars 2012, art. 9) «Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'État, la peine est portée à cinq ans d'emprisonnement et à (L. n° 2015-912 du 24 juill. 2015, art. 4) «150 000 €» d'amende.»

يتبين من المادة سالفة الذكر بأنه يعاقب على الدخول أو البقاء غير المشروع في أحد نظم المعالجة الآلية للمعلومات بعقوبة الحبس عامين، وغرامة قدرها 150 ألف يورو، وإذا ترتب على واقعة الدخول غير المشروع تعديل أو إلغاء أو إتلاف للبرامج أو نظم المعالجة الآلية للبيانات، وتشدد العقوبة إلى الحبس ثلاث سنوات وغرامة 100 ألف يورو، وتُشدد العقوبة إذا ارتكبت الأفعال سالفة الذكر على أحد الأنظمة الآلية للبيانات الشخصية المحفوظة على أجهزة الدولة.

ويعاقب كل من دخل عن طريق الاحتيال والغش إلى نظام معلوماتي (القانون رقم 1353-2014 الصادر 13 نوفمبر 2014) لاستخراج أو حيازة أو نسخ أو نقل، حذف أو تعديل عن طريق الاحتيال على البيانات التي تحتوي عليها (القانون رقم 575-2004 الصادر 21 يونيو 2004) عليها بالسجن خمس سنوات وغرامة 150 ألف يورو. وإذا وقعت الجريمة على موقع أو نظام المعالجة الآلية للبيانات الشخصية المحفوظة على أجهزة الدولة تشدد العقوبة لتصبح السجن لمدة سبع سنوات وغرامة قدرها 300 ألف يورو⁽¹⁾.

(1) Art. 323-3 "Le fait d'introduire frauduleusement des données dans un système de traitement automatisé (L. n° 2014-1353 du 13 nov. 2014, art. 16) « d'extraire, de détenir, de reproduire, de transmettre,» de supprimer ou de modifier frauduleusement les données qu'il contient est puni de (L. n° 2004-575 du 21 juin 2004, art. 45-III) «cinq ans» d'emprisonnement et de (L. n° 2015-912 du 24 juill. 2015, art. 4) «150 000 €» d'amende.

وتُشدد العقوبة في حالة ارتكاب الجريمة من قبل جماعة إجرامية مُنظمة, وذلك ما أقرته المادة (323 - 4-1) من قانون العقوبات بأن (القانون رقم 1353-2014 الصادر 13 نوفمبر 2014)⁽¹⁾ يُعاقب العقوبة بالسجن لمدة عشر سنوات وغرامة 300 ألف يورو (القانون رقم 912-2015 الصادر 24 يوليو 2015) إذا ارتكبت الجرائم المنصوص عليها في المواد 1-323 إلى 1-3-323 من قبل عصابات منظمة بدخول نظام المعالجة الآلية للبيانات الشخصية التي تم تخزينها على أجهزة الدولة"⁽²⁾.

(L. n° 2012-410 du 27 mars 2012, art. 9) «Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'État, la peine est portée à sept ans d'emprisonnement et à (L. n° 2015-912 du 24 juill. 2015, art. 4) «300 000 €» d'amende.»"

(1) – **JORF** n°0263 du 14 novembre 2014 page 19162, texte n° 5, LOI n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme .

(2) – **Art. 323-4-1** "(L. no 2014-1353 du 13 nov. 2014, art. 17) Lorsque les infractions prévues aux articles 323-1 à 323-3-1 ont été commises en bande organisée et à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'État, la peine est portée à dix ans d'emprisonnement et à (L. n° 2015-912 du 24 juill. 2015, art. 4) «300 000 €» d'amende".

ويعاقب بذات العقوبة في حالة المشاركة في جماعة إجرامية أنشأت بهدف ارتكاب
الجرائم السالفة الذكر (1)

ونص القانون الإماراتي في المادة (2) من المرسوم بقانون اتحادي رقم (5) لسنة
2012 على أن 1- يعاقب بالحبس والغرامة التي لا تقل عن مائة ألف درهم ولا
تزيد على ثلاثمائة ألف درهم أو بإحدى هاتين العقوبتين كل من دخل موقع
إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات، أو وسيلة تقنية معلومات،
بدون تصريح أو بتجاوز حدود التصريح، أو بالبقاء فيه بطريقة غير مشروعة. 2-
تكون العقوبة الحبس مدة لا تقل عن ستة أشهر والغرامة التي تقل عن مائة
وخمسين ألف درهم ولا تتجاوز سبعمائة وخمسون ألف درهم أو بإحدى هاتين
العقوبتين إذا ترتب على أي فعل من الأفعال المنصوص عليها في الفقرة (1) من
هذه المادة إلغاء أو حذف أو تدمير أو إفشاء، أو إتلاف أو تغيير أو نسخ أو نشر
أو إعادة نشر أي بيانات أو معلومات. 3- تكون العقوبة الحبس مدة لا تقل عن

(1) Art. 323-4 "La participation à un groupement formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs des infractions prévues par (L. n° 2004-575 du 21 juin 2004, art. 46-II) «les articles 323-1 à 323-3-1 [ancienne rédaction: les articles 323-1 à 323-3]» est punie des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée".

سنة واحدة والغرامة التي تقل عن مائتين وخمسين ألف درهم ولا تجاوز مليون درهم أو بإحدى هاتين العقوبتين إذا كانت البيانات أو المعلومات محل الأفعال الواردة في الفقرة (2) من هذه المادة شخصية.

ونص القانون الكويتي رقم (63) لسنة 2015 في شأن مكافحة جرائم تقنية المعلومات كذلك في المادة (2) على تجريم الدخول غير المشروع إلى جهاز حاسب آلي أو إلى نظامه أو إلى نظام معالجة إلكترونية للبيانات أو إلى نظام إلكتروني مؤمن إلى شبكة معلوماتية، إذا ترتب على الدخول إلغاء أو حذف أو إتلاف أو تدمير أو إفشاء أو تغيير أو إعادة نشر بيانات أو معلومات⁽¹⁾. كما

⁽¹⁾ نصت المادة (2) على أن "يعاقب بالحبس مدة لا تجاوز ستة أشهر وبغرامة لا تقل عن خمسمائة دينار ولا تجاوز ألفي دينار أو بإحدى هاتين العقوبتين، كل من ارتكب دخولاً غير مشروع إلى جهاز حاسب آلي أو إلى نظام معالجة إلكترونية للبيانات أو إلى نظام إلكتروني مؤتمت أو إلى شبكة معلوماتية. فإذا ترتب على هذا الدخول إلغاء أو حذف أو إتلاف أو تدمير أو إفشاء أو تغيير أو إعادة نشر بيانات أو معلومات، فتكون العقوبة الحبس مدة لا تجاوز سنتين والغرامة التي لا تقل عن ألفي دينار ولا تجاوز خمسة آلاف دينار أو بإحدى هاتين العقوبتين. فإذا كانت تلك البيانات أو المعلومات شخصية فتكون العقوبة الحبس مدة لا تجاوز ثلاث سنوات والغرامة التي لا تقل عن ثلاثة آلاف دينار ولا تجاوز عشرة آلاف دينار أو بإحدى هاتين العقوبتين.

ويعاقب بالحبس مدة لا تجاوز خمس سنوات وبغرامة لا تقل عن ثلاثة آلاف دينار ولا تجاوز عشرين ألف دينار أو بإحدى هاتين العقوبتين، كل من ارتكب أياً من الجرائم المنصوص عليها أعلاه أو سهل ذلك للغير وكان ذلك أثناء أو بسبب تأدية وظيفته".

جرمت الاتفاقية العربية لمكافحة تقنية المعلومات الدخول والبقاء والاتصال غير المشروع لكل أو جزء من تقنية المعلومات أو الاستمرار به⁽¹⁾.

والقانون العماني رقم (12) لسنة 2011 نصت المادة (3) من على أن يعاقب بالسجن مدة لا تقل عن شهر ولا تزيد على ستة أشهر وبغرامة لا تقل عن مائة ريال عماني ولا تزيد على خمسمائة ريال عماني أو بإحدى هاتين العقوبتين، كل من دخل عمدا ودون وجه حق موقعا إلكترونيا أو نظاما معلوماتيا أو وسائل تقنية المعلومات أو جزءا منها أو تجاوز الدخول المصرح به إليها أو استمر فيها بعد علمه بذلك . فإذا ترتب على ما ذكر في الفقرة الأولى إلغاء أو تغيير أو تعديل أو تشويه أو إتلاف أو نسخ أو تدمير أو نشر أو إعادة نشر بيانات أو معلومات إلكترونية مخزنة في النظام المعلوماتي أو وسائل تقنية المعلومات أو تدمير ذلك النظام أو وسائل تقنية المعلومات أو الشبكة المعلوماتية أو إلحاق ضرر بالمستخدمين أو المستفيدين، تكون العقوبة السجن مدة لا تقل عن ستة أشهر ولا تزيد على سنة وغرامة لا تقل عن خمسمائة ريال عماني ولا تزيد على ألف ريال عماني أو بإحدى هاتين العقوبتين. فإذا كانت البيانات أو المعلومات المنصوص عليها في الفقرة الثانية شخصية تكون العقوبة السجن مدة لا تقل عن سنة ولا تزيد

(1) المادة السادسة جريمة الدخول غير المشروع: 1- "الدخول أو البقاء وكل اتصال غير مشروع مع كل أو جزء من تقنية المعلومات أو الاستمرار به. 2- تشدد العقوبة إذا ترتب على هذا الدخول أو البقاء أو الاتصال أو الاستمرار بهذا الاتصال: (أ) محو أو تعديل أو تشويه أو نسخ أو نقل أو تدمير للبيانات المحفوظة وللأجهزة والأنظمة الإلكترونية وشبكات الاتصال وإلحاق الضرر بالمستخدمين والمستفيدين. (ب) الحصول على معلومات حكومية سرية."

على ثلاث سنوات وغرامة لا تقل عن ألف ريال عماني ولا تزيد على ثلاثة آلاف ريال عماني أو بإحدى هاتين العقوبتين.

يتبين لنا أن كافة التشريعات المنظمة لجرائم تقنية المعلومات والاتفاقية العربية لمكافحة جرائم تقنية المعلومات نصوا على تجريم صور الدخول غير المشروع إلى موقع إلكتروني، أو نظام معلومات إلكتروني، أو شبكة معلومات، أو وسيلة تقنية معلومات، وتشدّد العقوبة إذا ترتب على الدخول الإلغاء أو الحذف أو التدمير أو الإفشاء، أو الإتلاف أو التغيير أو النسخ أو النشر أو إعادة النشر لأيّ بيانات أو معلومات، وتصبح العقوبة أشد إذا كان الموقع والبيانات شخصية، لذلك نرى ضرورة النص صراحة في القانون رقم 175 لسنة 2018 على تجريم الدخول غير المشروع لمواقع التواصل الاجتماعي.

الركن المادي:

لم يعرف المشرع المصري الدخول غير المشروع، علا خلاف القانون الكويتي رقم (63) لسنة 2015 عرف الدخول غير المشروع بأنه النفاذ المتعمد غير المشروع لأجهزة وأنظمة الحاسب الآلي أو لنظام معلوماتي أو شبكة معلوماتية أو موقع إلكتروني من خلال اختراق وسائل وإجراءات الحماية لها بشكل جزئي أو كلي لأي غرض كان بدون تفويض في ذلك أو تجاوز للتفويض الممنوح⁽¹⁾.

(1) المادة الأولى من القانون رقم (63) لسنة 2015.

ويمكننا تعريف الدخول غير المشروع بأنه الاختراق العمدي غير المشروع لأجهزة وأنظمة الحاسب الآلي أو لنظام تقنية المعلومات أو شبكة معلوماتية أو موقع إلكتروني أو مواقع التواصل الاجتماعي من خلال اختراق وسائل وإجراءات الحماية بشكل جزئي أو كلي لأي غرض، بدون تصريح أو تجاوز للتفويض المصرح به.

عقوبة الشروع:

نصت المادة 40 من القانون رقم 175 لسنة 2018 على أن كل من شرع في ارتكاب الجرائم المنصوص عليها بالقانون، يعاقب بما لا يجاوز نصف الحد الأقصى للعقوبة المقررة للجريمة.

وقد جعل المشرع الفرنسي عقوبة الشروع ذات عقوبة الجريمة، وذلك ما أكدته المادة (7-323) من قانون العقوبات، نصت بأن يعاقب على الشروع في الجرائم المنصوص عليها (القانون رقم 2004-575 الصادر 21 يونيو 2004) في المواد 1-323 حتى 1-3-323 بذات العقوبات المنصوص عليها للجريمة⁽¹⁾.

نعتقد أن المشرع الفرنسي أحسن صنعا من المشرع المصري، لأنه شدد عقوبة الشروع وجعلها ذات عقوبة الجريمة.

العقوبات التكميلية:

(1) – **Art. 323-7** " La tentative des délits prévus par (L. n° 2004-575 du 21 juin 2004, art. 46-II) «les articles 323-1 à 323-3-1» est punie des mêmes peines".

نص القانون رقم 175 لسنة 2018 على العقوبات التبعية في المادة (38) على أن "مع عدم الإخلال بحقوق الغير حسن النية، على المحكمة في حالة الحكم بالإدانة في أي جريمة من الجرائم المنصوص عليها في هذا القانون، أن تقضى بمصادرة الأدوات والآلات والمعدات والأجهزة مما لا يجوز حيازتها قانوناً، أو غيرها مما يكون قد استخدم في ارتكاب الجريمة، أو سهل أو ساهم في ارتكابها".

ونصت المادة (39) من القانون أن للمحكمة إذا قضت بالإدانة على أحد الموظفين العموميين، لارتكابه جريمة من الجرائم المنصوص عليها في هذا القانون، أثناء وبسبب تأديته لوظيفته، أن تقضى بعزله مؤقتاً من وظيفته، إلا في الحالات المشار إليها في المادة (35) من هذا القانون فيكون العزل وجوبياً.

ونص القانون الفرنسي على أن يخضع الأشخاص المدانين بالجرائم المنصوص عليها للعقوبات التكميلية لتالية:

1- المنع من ممارسة الحقوق المدنية لمدة تصل إلى خمس سنوات، وفقاً لأحكام المادة 131-26 من قانون العقوبات.

2- المنع من تولي مناصب عامة أو القيام بالنشاط الاجتماعي أو وظيفي الذي بممارسته أو بمناسبة ارتكبه الجريمة لمدة أقصاها خمس سنوات 131-27.

3- مصادرة الأشياء الذي استخدمت أو أعدت لارتكاب الجريمة أو الناتج عن الجريمة، باستثناء المواد الخاضعة للاسترداد، المادة 131-21 من قانون العقوبات.

- 4- إغلاق المنشأة أو المؤسسة التي استخدمت لارتكاب الجريمة لمدة خمس سنوات أو أحد أو أكثر من المؤسسات للشركة المستخدمة في ارتكاب الجريمة؛ المادة 131-33 من قانون العقوبات.
- 5- استبعاد المشتريات والتوريدات لمدة لا تزيد عن خمس سنوات، المادة 131-34 من قانون العقوبات.
- 6- حظر إصدار أو سحب شيكات لمدة خمس سنوات، المادة 131-19 من قانون العقوبات.
- 7- إشهار أو نشر القرار الذي اتخذ وفقا للمادة 131-35 من قانون العقوبات⁽¹⁾.

(1) – **Art. 323-5** Les personnes physiques coupables des délits prévus au présent chapitre encourent également les peines complémentaires suivantes:

1° L'interdiction, pour une durée de cinq ans au plus, des droits civiques, civils et de famille, suivant les modalités de l'article 131-26;

2° L'interdiction, pour une durée de cinq ans au plus, d'exercer une fonction publique ou d'exercer l'activité professionnelle ou sociale dans l'exercice de laquelle ou à l'occasion de laquelle l'infraction a été commise; — Pén. 131-27.

3° La confiscation de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit, à l'exception des objets susceptibles de restitution; — Pén. 131-21.

4° La fermeture, pour une durée de cinq ans au plus, des établissements ou de l'un ou de plusieurs des établissements de

الإعفاء أو التخفيف من العقوبة:

نصت المادة (41) من القانون رقم 175 لسنة 2018 على أن "يعفى من العقوبات، المقررة للجرائم المنصوص عليها في هذا القانون، كل من بادر من الجناة أو الشركاء إلى إبلاغ السلطات القضائية أو السلطات العامة بما يعلمه عنها قبل البدء في تنفيذ الجريمة وقبل كشفها.

ويجوز للمحكمة الإعفاء من العقوبة أو التخفيف منها إذا حصل البلاغ بعد كشف الجريمة وقبل التصرف في التحقيق فيها، إذا مكن الجاني أو الشريك في أثناء التحقيق السلطات المختصة من القبض على مرتكبي الجريمة الآخرين، أو على ضبط الأموال موضوع الجريمة، أو أعان أثناء البحث والتحقيق على كشف الحقيقة فيها، أو على القبض على مرتكبي جريمة أخرى مماثلة لهذا النوع والخطورة. ولا يخل حكم هذه المادة، بوجود الحكم برد المال المتحصل من الجرائم المنصوص عليها بالقانون".

l'entreprise ayant servi à commettre les faits incriminés; — Pén. 131-33.

5° L'exclusion, pour une durée de cinq ans au plus, des marchés publics; — Pén. 131-34.

6° L'interdiction, pour une durée de cinq ans au plus, d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés; — Pén. 131-19.

7° L'affichage ou la diffusion de la décision prononcée dans les conditions prévues par l'article 131-35".

العدوى بالفيروسات عبر مواقع التواصل الاجتماعي:

قد يكون الدخول مشروعاً، إلا أن الهدف منه يكون بغاية الإضرار بأجهزة الغير عن طريق إرسال فيروسات⁽¹⁾، يعتبر من أخطر الاعتداءات على وسائل التقنية، وتسبب العدوى عن طريق الفيروسات والبرمجيات الخبيثة في إتلاف أجهز الكمبيوتر، أو تدمير البرامج، أو إتلاف البيانات أو المعلومات المخزنة⁽²⁾.

فقد نصت المادة 17 من القانون رقم 175 لسنة 2018 على جريمة الاعتداء على سلامة البيانات والمعلومات والنظم المعلوماتية، حيث يعاقب بالحبس مدة لا تقل عن سنتين وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز خمسمائة ألف جنيه، أو بإحدى هاتين العقوبتين كل من أتلّف أو عطل أو عدل مسار أو ألغى كلياً أو جزئياً، متعمداً وبدون وجه حق، البرامج والبيانات أو المعلومات المخزنة، أو

(1) الفيروسات عبارة عن برمجيات مشفرة للحاسب الآلي مثل أي برمجيات أخرى، يتم تصميمها بهدف محدد وهو إحداث أكبر ضرر ممكن بأنظمة الحاسب الآلي، وتتميز بقدرتها على ربط نفسها بالبرامج الأخرى وإعادة إنشاء نفسها حتى تبدو وكأنها تتكاثر ذاتياً، بالإضافة إلى قدرتها على الانتشار من نظام إلى آخر، إما بواسطة قرص ممغنط أو عبر شبكة الاتصالات بحيث يمكنها أن تنتقل عبر الحدود من أي مكان إلى آخر في العالم. د/حسين بن سعيد بن سيف الغافري، السياسة الجنائية في مواجهة جرائم الإنترنت، دراسة مقارنة، رسالة دكتوراه كلية حقوق جامعة عين شمس، دون سنة، ص315.

(2) – **Jacques Francillon**: De diverses variétés de piratages, RSC, N° 01 du 16/03/1998, p.138 et s;

: Piratage audiovisuel. Captation frauduleuse de programmes de télévision cryptée à péage, RSC, N° 01 du 16/06/2014, p.117.

المعالجة، أو المولدة أو المخلفة على أي نظام معلوماتي وما في حكمه، أيا كانت الوسيلة التي استخدمت في الجريمة.

فقد جرمت كافة التشريعات المنظمة لجرائم تقنية المعلومات الدخول غير المصرح وإتلاف أو تعطيل البرامج ومنها القانون المصري، كما سبق أن ذكرنا، إلا أنها لم تتناول جريمة إرسال الفيروسات عبر الإنترنت، وخاصة عبر مواقع التواصل الاجتماعي.

فإن القائمين على نشر الفيروسات قد لا يدخلون إلى تلك المواقع ويكتفون بإرسال تلك الفيروسات عبر الإنترنت فقط، كما أن الدخول إلى النظام لا يترتب عليه الإلغاء أو الحذف أو التدمير أو الإفشاء أو الإتلاف أو التغيير أو النسخ أو النشر أو إعادة النشر لأي بيانات أو معلومات فقط، وإنما قد ينجم عنه تعديل في البيانات المخزنة ألياً، أو ضعف أداء هذا النظام.

لذلك نرى ضرورة التوسع في نطاق التجريم ليشمل إرسال أي بيانات إلكترونية تحتوي على فيروسات ضارة من أي نوع، أو تعديل البيانات الواردة في النظام، أو ضعف أداء هذا النظام، وعدم قصر حالات التجريم على دخول الجاني إلى النظام المعلوماتي بأكمله؛ إذ يكفي الدخول إلى جزء من موقع إلكتروني، أو نظام معلومات إلكتروني، أو شبكة معلومات، أو أي وسيلة من وسائل تقنية معلومات.

الفرع الثالث

جرائم النشر الإلكتروني عبر مواقع التواصل الاجتماعي

يتوقف النظام القانوني للمسئولية الجنائية في الجرائم الناشئة عن إساءة استخدام مواقع التواصل الاجتماعي على التكييف القانوني للقائم بالتشغيل.

أولاً: المقصود بالناشر الإلكتروني:

لم ينص القانون رقم 175 لسنة 2018 المصري، والقانون المقارن تعريف لناشر المحتوى في جرائم النشر الإلكتروني بخلاف "مقدمي خدمات استضافة المواقع"، نصت المادة (6) من القانون الفرنسي بشأن الاقتصاد الرقمي (CEN) المعدل بمقتضى القانون 444-2016 الصادر 13 إبريل 2016⁽¹⁾ على أن مقدمي خدمات الاستضافة هم الأشخاص الطبيعيون أو الاعتباريون القائمون على توصيل خدمات الاتصال للجمهور عبر الإنترنت، وتخزين إشارات أو كتابات أو صور أو أصوات، أو رسائل من أي نوع، تصدر عن المستخدمين من تلك الخدمات. وبالتالي يترك سلطة تقديرية في تحديد المراد بالناشر الإلكتروني، وقد عرف التقرير الصادر عن الجمعية الوطنية الفرنسية الناشرين بأنهم الأشخاص الذين يقومون

⁽¹⁾-JORF n°0088 du 14 avril 2016, texte n° 1 , LOI n° 2016-444 du 13 avril 2016 visant à renforcer la lutte contre le système prostitutionnel et à accompagner les personnes prostituées .

بصياغة المعلومات أو تحريرها أو نشرها أو إعادة نشرها أو وضعها على مواقع التواصل الاجتماعي⁽¹⁾.

قد يكون الناشر الإلكتروني مدير تحرير الموقع أي الذي قام بإنشاء صفحة الويب، وقد يكون شخصاً آخر قام بنشر المحتوى على الموقع، أو كتب تعليقاً، أو أرسل نصاً، أو رسالة، أو مقطع فيديو، أو حتى رسم صورة، وعليه يخرج من نطاق الناشر الإلكتروني الأشخاص المنوط بهم توصيل خدمات الاتصال مباشرة بالإنترنت⁽²⁾، وتخزين المعلومات؛ فهؤلاء مزودو خدمات استضافة، وليسوا ناشرين⁽³⁾.

وبذلك يتبين أن للناشر الإلكتروني مفهوماً واسعاً، إذ يشمل من قام بإنشاء صفحة التواصل الاجتماعي، وسمح للأشخاص بالدخول إليها بعد تسجيل بياناتهم، ومن

(1)– Rapport d'information de l'Assemblée Nationale sur la mise en application de la loi no.2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, présenté par M. Jean Dionis du Séjour et Corinne Erhel. Ce.

rapport est disponible sur: <http://www.assemblee-nationale.fr/13/rap-info/i0627.asp>

(2) Tribunal de grande instance de Nanterre, 1re ch, 25-06-2009, n° 08/05405.

(3) **Jérôme Huet**: Site internet, flux RSS, responsabilité du rediffuseur, Recueil Dalloz, N° 15 du 15/04/2010, p.946.

قام بتدوين المحتوى وصياغته، ووضعه على الموقع، أو أرسله عبر الشبكة إلى مستخدمين آخرين.

ولم يضع المشرعان الإماراتي والكويتي تعريفاً محدداً للناشر الإلكتروني في جرائم النشر، فاكتمت في المادة الثانية من القانونين في شأن جرائم تقنية المعلومات بالنص على معاقبة كل من دخل موقعاً إلكترونياً أو نظام معلومات إلكترونياً أو شبكة معلومات، أو وسيلة تقنية معلومات، من دون تصريح أو بتجاوز حدود التصريح، أو بالبقاء فيه بصورة غير مشروعة.

فالناشر الإلكتروني هو كل شخص طبيعي أو اعتباري قام بإنشاء مواقع على الشبكة، وسمح فيها بإضافة أشخاص وتلقى منهم البرامج والمعلومات، وكذلك من قام بتدوين المحتوى وصياغته، أو وضعه، أو إرساله إلى الموقع الإلكتروني، أو إحدى وسائل تقنية المعلومات، وجعله متاحاً لمستخدمي الإنترنت.

ثانياً: جرائم النشر الإلكتروني:

قد تقع جرائم نشر البيانات أو المعلومات أو إعادة نشرها من المستخدمين لمواقع التواصل الاجتماعي، أو من شخص قام بالنشر أو إعادة النشر، أو بسبب تأدية عمله، كأن يستغل الأخير شبكة الإنترنت في الجهة التي يعمل بها ويقوم بنشر بيانات أو معلومات أو إعادة نشرها، سواء كانت هناك صلة بين هذه المعلومات والجهة التي يعمل بها أم لا.

وفي هذا الصدد نصت المادة (8) من القانون الكويتي رقم (63) لسنة 2015 في شأن مكافحة جرائم تقنية المعلومات على أن "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"

واشترط المشرع وفقاً للمادة الثالثة من القانون الإماراتي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات أن يكون عمل الشخص في تلك الجهة قد سهل له نشر بيانات أو معلومات أو إعادة نشرها، فالمصلحة المحمية جنائياً هي عدم استغلال تلك الجهة في نشر بيانات أو معلومات.

ويلاحظ أن المشرع الإماراتي لم يشرط في المواد " 2، 3، 4" أن تتطوي البيانات، أو المعلومات التي يتم نشرها على وقائع تتضمن الإساءة إلى مستخدمين آخرين، أو التحريض على ارتكاب جرائم باستغلال هذه المواقع؛ فالمشرع يستهدف من ذلك حماية خصوصية مستخدمي مواقع التواصل الاجتماعي وحقوق النشر المملوكة لهم.

نعتقد أن السياسة التشريعية التي انتهجها المشرع الإماراتي في جرائم النشر الإلكتروني أفضل من سياسة المشرع الكويتي، حيث اعتمد المشرع الإماراتي على وضع نصوص مستقلة تتناول جرائم الإساءة إلى آخرين كجريمة نشر أو إعادة نشر أرقام أو بيانات بطاقة ائتمانية أو إلكترونية أو أرقام أو بيانات حسابات مصرفية تعود للغير أو أي وسيلة أخرى من وسائل الدفع الإلكتروني⁽¹⁾. أو جرائم نشر أو بث معلومات أو أخبار أو رسوم كرتونية أو أي صور أخرى، من شأنها تعريض أمن الدولة ومصالحها العليا للخطر أو المساس بالنظام العام⁽²⁾. أو جرائم نشر معلومات أو أخبار أو بيانات أو شائعات على موقع إلكتروني أو أي شبكة معلوماتية أو وسيلة تقنية معلومات بقصد السخرية أو الإضرار بسمعة أو هيبة أو مكانة الدولة أو أي من مؤسساتها أو رئيسها أو نائبه أو حكام الإمارات أو أولياء عهدهم أو نواب حكام الإمارات أو علم الدولة أو السلام الوطني أو شعارها أو نشيدها الوطني أو رموزها⁽³⁾.

ووضع المشرع الإماراتي نصوص تُجرّم نشر البيانات أو المعلومات التي تهدف إلى التحريض على ارتكاب جرائم بعينها، كما لو نشر الجاني، أو أعاد نشر مواد إباحية أو أنشطة للقمار، وكل ما من شأنه المساس بالآداب العامة عن طريق

(1) الفقرة الرابعة من المادة (12) من المرسوم بقانون اتحادي في شأن جرائم تقنية المعلومات.

(2) المادة (28) من المرسوم بقانون اتحادي في شأن جرائم تقنية المعلومات.

(3) المادة (29) من المرسوم بقانون اتحادي في شأن جرائم تقنية المعلومات.

الشبكة المعلوماتية⁽¹⁾. أو وقع النشر بقصد الاتجار في البشر أو الأعضاء البشرية، أو التعامل فيها بصورة غير مشروعة⁽²⁾، أو بهدف إثارة الفتنة أو الكراهية أو العنصرية أو الطائفية أو الإضرار بالوحدة الوطنية أو السلم الاجتماعي أو الإخلال بالنظام العام أو الآداب العامة، أو الاتجار أو الترويج للأسلحة النارية أو الذخائر أو المتفجرات في غير الأحوال المصرح بها قانوناً⁽³⁾، أو نشر معلومات على الشبكة المعلوماتية أو وسيلة تقنية معلومات، وذلك لجماعة إرهابية أو أي مجموعة أو جمعية أو منظمة أو هيئة غير مشروعة بقصد تسهيل الاتصال بقياداتها أو أعضائها، أو لاستقطاب عضوية لها، أو ترويج أو تحبيذ أفكارها، أو تمويل أنشطتها، أو توفير المساعدة الفعلية لها، أو بقصد نشر أساليب تصنيع الأجهزة الحارقة أو المتفجرات، أو أي أدوات أخرى تستخدم في الأعمال الإرهابية⁽⁴⁾.

ويتضح مما سبق أن المشرع الإماراتي لم يشترط في جرائم النشر الإلكتروني صفة معينة في مرتكبها، فهي تقع بمجرد نشر البيانات أو المعلومات التي تخص آخرين، وقد يستغل الجاني النشر الإلكتروني في الإساءة إلى الآخرين أو التحريض على ارتكاب جرائم، بينما قد يكون الناشر الإلكتروني مجنباً عليه عندما يقع التعدي على حقوق النشر المحفوظة له.

(1) المادة (17) من المرسوم بقانون اتحادي في شأن جرائم تقنية المعلومات.

(2) المادة (23) من المرسوم بقانون اتحادي في شأن جرائم تقنية المعلومات.

(3) المادة (25) من المرسوم بقانون اتحادي في شأن جرائم تقنية المعلومات.

(4) المادة (26) من المرسوم بقانون اتحادي في شأن جرائم تقنية المعلومات.

وكذلك من يتلقى تلك الرسائل على صفحته الشخصية أو على الموقع باعتبار أنه مصرح له بذلك، فضلاً عن أن شرعية الدخول متوافرة في حقه. ولا شك في أن ذلك يترتب عليه نتائج سيئة؛ لأن الناشر الإلكتروني قد يكون مدير تحرير للموقع الذي قام بإنشاء صفحة، أو منتدى على الموقع بطريق مشروع، ثم سمح للمستخدمين بالدخول إليها ونشر البيانات والمعلومات على الموقع للمستخدمين الآخرين.

ومن ثم، فإذا كانت هذه البيانات تتطوي على جريمة أصبح مدير تحرير الموقع مسؤولاً عنها، لأنه سمح بنشرها على موقعه، ومن ثم تتعدد المسؤولية الجنائية في حقه عما تضمنه هذا المحتوى. في حين أنه استناداً إلى المادة السالفة الذكر لن تعاقب؛ لأنه لم يدخل إلى الموقع من دون تصريح، ولم يتجاوز حدود التصريح، أو بقي في الموقع بصورة غير مشروعة. ومن ناحية أخرى فالشخص الذي يقوم بتدوين المحتوى أو كتابته أو صياغته، أو إرساله إلى مدير تحرير الموقع، لا يعد في مفهوم المادة الثانية ناشراً لأنه لم يدخل إلى الموقع بطريق غير مشروع، بينما المستقر عليه أنه يعد ناشراً إلكترونياً أيضاً من قام بإنشاء أو كتابة، أو تدوين، أو صياغة المحتوى من الأصل، أو من توافر لديه قدرة التحكم والسيطرة على المحتوى قبل وضعه على الإنترنت.

وكذلك الشخص الذي يقوم بإرسال رسائل نصية عبر الهاتف المحمول أو الإنترنت إلى موقع التواصل الاجتماعي لا يعد ناشراً إلكترونياً، لأنه لم يدخل إلى الموقع،

وبالتالي قد يرسل شخص مقطع فيديو تم تصويره بالهاتف المحمول يحرض على العنف أو يهدد أمن الدولة وسلامتها إلى هذه المواقع دون أن يدخل إليها بالمفهوم التقني البحت، ولا محالة حينئذٍ من اعتباره ناشراً إلكترونياً، ومن ثم نرى ضرورة عدم ربط مسألة الدخول للموقع بغير تصريح بواقعة نشر البيانات، والتي قد تتحقق بصورة أو بأخرى وبصرف النظر عن كيفية الدخول.

نعتقد ضرورة تعديل القانون المصري رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات، على معاقبة كل من أنشأ على مواقع التواصل الاجتماعي صفحات تستغل في نشر أو إعادة نشر أو كتابة أو تدوين أو صياغة معلومات، أو بيانات، أو صور، أو أفلام، أو مستندات، أو أرقام، أو حروف، أو رموز، أو إشارات وغيرها، أو جعلها متاحة لمستخدمي الإنترنت، أو سهل للغير ذلك. كما يعاقب بالعقوبة ذاتها كل من قام بصياغة أو كتابة أو تدوين أو إرسال شيء مما ذكر، وتكون العقوبة السجن المؤبد إذا كانت تلك المعلومات، أو البيانات، أو الصور، أو الأفلام، أو المستندات، أو الأرقام، أو الحروف، أو الرموز، أو الإشارات تتصل بأسرار الدولة العسكرية أو الأمنية أو تهدد مصالحها الاقتصادية.

كما نرى ضرورة العمل على استثمار إيجابيات مواقع التواصل الاجتماعي، والتي من أبرزها الاستخدامات للأغراض التعليمية والاستخدامات الحكومية والتجارية، والحذر من سلبياتها كنشر أفكار هدامة وعمل تجمعات مخالفة للقيم والأخلاق.

ثالثاً: تحديد المسؤولية الجنائية في جرائم النشر الإلكتروني:

لتحديد المسؤولية الجنائية في جرائم النشر الإلكتروني تقتضي تناول أمرين: الأول، أوجه التمييز بين الناشر ومزود خدمات الاستضافة. والثاني، المسؤولية الجنائية عن جرائم النشر الإلكتروني.

التمييز بين الناشر ومزود خدمات الاستضافة:

إذا كان مزود خدمات الاستضافة هو المسئول عن توفير خدمة الاتصالات عبر الإنترنت للجمهور، أو يتيح تخزين المعلومات التي ترد إليه من أي شخص أسهم في إنشاء محتوى، أو صياغته، فالناشر هو ذلك الشخص الذي إما أن يُسهل نشر البيانات على الموقع باعتباره مدير تحرير لهذا الموقع، وإما أن يقوم بتدوين المحتوى وصياغته.

فالذي يميز بين المضيف والناشر هو أن الأخير تكون له السيطرة على المحتوى، والتحكم في بياناته، بخلاف المضيف حيث تقتصر مهمته على حد توفير خدمات الاتصال للجمهور، وحفظ البيانات وتخزينها، ومن ثم لا تكون له علاقة بإنشاء صفحات التواصل الاجتماعي، أو مضمون المحتوى.

تحديد شخص القائم بالنشر الإلكتروني:

توجد صعوبة في تحديد القائم بالنشر الإلكتروني، فمعظم مستخدمي مواقع التواصل الاجتماعي يدخلون إلى تلك المواقع باستخدام أسماء وهمية، كما أن الشخص الذي

قام بإنشاء المنتدى أو الصفحة قد لا يتوافر لديه العلم بما تم نشره على الصفحة لسبب أو لآخر، وحتى يتسنى إيجاد الحلول لذلك، يتعين الالتزام بالتالي:

يجب على مدير تحرير الموقع رصد ما يتم نشره على الموقع ومراقبته، باعتباره هو الذي قام بإنشاء صفحة التواصل على الموقع، ومن ثم تتعدد المسؤولية في حقه عن نشر عبارات أو معلومات أو بيانات تشكل جريمة يعاقب عليها قانوناً إذ يُفترض في حقه العلم بما يتم نشره، إلى جانب مسؤولية المدون أيضاً، باعتبار أنه تتوافر له السيطرة على المحتوى، ومن ثم يستطيع أن يتحكم في المعلومات الواردة فيه، سواء عند إنشائه، أو كتابته، أو صياغته. أما إذا انتفى القصد الجنائي لدى مدير التحرير فلا محل لمساءلته عن الجريمة، وإن كان ذلك لا يحول دون توافر المسؤولية عن جرائم النشر بوصفها جريمة غير عمدية إذا ثبت أن مدير تحرير الموقع أهمل في واجب الرقابة والإشراف لما يتم نشره، باعتبار أن من واجبه بذل العناية اللازمة في مراقبة هذه المعلومات ورصدها.

نعتقد أنه يجب إيجاد تقنية فنية تسمح لمن قام بإنشاء صفحات على موقع التواصل الاجتماعي بمراقبة ما يتم نشره على الموقع، حتى نتجنب ما يمكن أن يثار من أن مدير التحرير لم يعلم بما تم نشره على الموقع، سواء كان ذلك نتيجة زيادة أعداد المستخدمين، أو كثرة البيانات المطروحة.

التزامات الناشر الإلكتروني:

- 1- يلتزم مدير تحرير الموقع الذي أنشأ صفحة على موقع التواصل الاجتماعي بأن يُدرج اسم موقعه، ويحدد هويته على شبكة الإنترنت لإمكانية التعرف عليه بسهولة.
- 2- يكون لمدير التحرير والناشر الحق في تعديل كل ما يتضمنه المحتوى من بيانات مخالفة، أو ما يشكل مخالفة لشروط الاستخدام تعديلاً كلياً أو جزئياً.
- 3- يجب على مدير تحرير الموقع أن يحدد شروط استخدام هذا الموقع، وأن يقيد استخدامه في أغراض التبادل الثقافي، والعلمي، والاجتماعي دون استغلاله في ارتكاب جرائم.
- 4- عدم قبول دخول المستخدمين إلى هذه المواقع إلا بالهوية الحقيقية دون استخدام هوية مزورة، مع تحذير المستخدم بأن الدخول بهوية غير حقيقية، أو وهمية جريمة مُعاقبٌ عليها قانوناً.
- 5- يتعين الإبلاغ عن إساءة استخدام مواقع التواصل الاجتماعي ضد الأطفال والقُصّر.
- 6- يجب على مدير تحرير الموقع في حالات النشر عن طريق الوسائل الإلكترونية، الالتزام بتوفير المعلومات العامة، وتحديد هوية مؤلفي المحتوى، ودور النشر.

وهناك التزامات قانونية يخضع لها الناشر، وعند الخروج عن هذه الالتزامات تتوافر المسؤولية الجنائية في حقهم⁽¹⁾، وقد اعتمد المجلس الدستوري الفرنسي ذلك القانون من قبل الجمعية الوطنية ومجلس الشيوخ في 30 يونيو 2006، ونص على غرامة تبدأ من 300 ألف يورو إضافة إلى ثلاث سنوات سجن لأي شخص يقوم بنشر أو يزود الجمهور ببرامج تحرير غير مصرح بها. وتصل العقوبة إلى السجن 6 أشهر والغرامة 30 ألف يورو لأي شخص يوزع أو يسهل توزيع البرمجيات بمخالفة تدابير الحماية التقنية (DRM) لإدارة الحقوق الرقمية⁽²⁾.

رابعاً: عقوبة جريمة النشر الإلكتروني:

عاقب المشرعون المصري والفرنسي والإماراتي والكويتي كل من يقوم بالدخول غير المشروع إلى نظام معلومات إلكتروني أو شبكة معلومات، أو وسيلة تقنية

(1) Frédéric Pollaud-Dulian: Exception de copie privée, RTD, N° 02 du 15/06/2007, p.357 et s.

(2) Frédéric Pollaud-Dulia: Protection juridique des mesures techniques de protection ou d'information. Echanges de « pair à pair ». Téléchargement illicite. Sanctions pénales. Logiciels d'échanges. Autorité de régulation des mesures techniques, RTD Co, N° 02 du 15/06/2007, p.346 et s. Frédéric Pollaud-Dulian: Programmes d'ordinateur. Épuisement du droit de distribution. Revente d'occasion de copies. Supports physiques qui ne sont pas d'origine. Exceptions au droit de reproduction du logiciel, RTD Com, N° 04 du 19/01/2017, p.741et s.

معلومات، دون تصريح أو بتجاوز حدود التصريح، أو بالبقاء فيه بصورة غير مشروعة. أما إذا ترتب على ذلك نشر أو إعادة نشر أي من هذه البيانات أو المعلومات فيُعد ذلك ظرفاً مشدداً يتم بمقتضاه تشديد العقوبة. وتشدد العقوبة إذا وقعت الجريمة من الجاني بمناسبة أو بسبب تأدية عمله.

وإذا انتفى لدى الجاني القصد الجنائي فلا يعاقب عن تلك الجريمة، كأن ينتفي لديه العلم بنشر البيانات، أو يجهل حقيقة ما يفعله، أو حكم القانون فيه، أو يغلط في أيهما، فالجهل أو الغلط في الوقائع ينفيان القصد الجنائي.

الفرع الرابع

المسئولية الجنائية لمقدمي الخدمات عبر مواقع التواصل الاجتماعي

أولاً: تعريف مزود الخدمة:

عرف المشرع المصري في القانون رقم 175 لسنة 2018 مقدم الخدمة في المادة الأولى بأنه أي شخص طبيعي أو اعتباري يزود المستخدمين بخدمات تقنيات المعلومات والاتصالات، ويشمل ذلك من يقوم بمعالجة أو تخزين المعلومات بذاته أو من ينوب عنه في أي من تلك الخدمات أو تقنية المعلومات. وعرفت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات مزود الخدمة بأنه أي شخص طبيعي أو معنوي عام أو خاص يزود المشتركين بالخدمات للتواصل بواسطة تقنية المعلومات، أو يقوم بمعالجة أو تخزين المعلومات نيابة عن خدمة الاتصالات أو مستخدميها⁽¹⁾.

فمقدم خدمة التقنية هو كل شخص طبيعي، أو معنوي عام أو خاص يعمل على توفير خدمات الاتصال للجمهور، أو يقوم بمعالجة أو تخزين المعلومات، ويلتزم بالإبقاء على البيانات التي تمكّن من التعرف إلى مدير تحرير الموقع.

(1) الفقرة الثالثة من المادة (2) من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، الجريدة الرسمية، العدد (46) الصادر 13 نوفمبر 2014، قرار رئيس الجمهورية بشأن انضمام جمهورية مصر العربية إلى الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، الموقعة في القاهرة بتاريخ 21 ديسمبر 2010.

ويمكننا تعريف مزود الخدمة بأنه كل شخص طبيعي أو معنوي يزود المستخدمين بخدمات التواصل بواسطة تقنية المعلومات ويشمل ذلك من يقوم بمعالجة أو تخزين المعلومات نيابة عن مقدم خدمة الاتصالات أو المعلومات.

وتتعدد المسؤولية الجنائية عن جرائم النشر على مديري التحرير أو الناشرين، فهؤلاء هم المسؤولون عن الجرائم التي يرتكبها المدونون كونهم المنوط بهم مراجعة تلك البيانات وصياغتها قبل وضعها على صفحات الويب وشبكة الإنترنت. أما مقدمو خدمات الاستضافة فلا يستطيعون مراقبة البيانات التي تنشر على الشبكة، ويترتب على ذلك، أن مزود خدمة الاستضافة يلتزم بتخزين البيانات وجعلها متاحة للمستخدمين عبر شبكة الإنترنت فقط، ولا تكون له علاقة بمضمون المحتوى⁽¹⁾.

وتتعدد مسؤولية مزودي خدمات الاستضافة في حالتين:

1 - إذا توافر لديهم العلم الفعلي بالطبيعة غير المشروعة للمحتوى، ولم يخطرأ السلطات أو يتصرفوا فوراً لإزالة البيانات، أو جعل الوصول إليها مستحيلاً , المادة 6 /2 من القانون الفرنسي بشأن الاقتصاد الرقمي⁽²⁾.

(1) – **Jacques Francillon:** Application à la télématique et à l'Internet des règles de responsabilité propres au droit de la presse et de la communication audiovisuelle, RSC, N° 03 du 15/09/1999, p.607 et s.

(2) – **Présidence et mot d'accueil:** Rôle et responsabilité des plateformes en ligne: approche(s) transversale(s) ou approches sectorielles ?, Master 2 « Droit du commerce électronique et de l'économie numérique », Ecole de droit de la Sorbonne, Université

2- إذا لم يُبقوا على البيانات التي يمكن من خلالها التعرف إلى مدير تحرير الموقع والمدون⁽¹⁾.

ثانياً: التزامات مزودي خدمة الاستضافة:

وضع المشرع المصري في القانون رقم 175 لسنة 2018 التزامات وواجبات على مقدم الخدمة، في المادة (2) على النحو التالي:

أولاً: مع عدم الإخلال بالأحكام الواردة بهذا القانون وقانون تنظيم الاتصالات رقم 10 لسنة 2003 المشار إليه، يلتزم مقدمو الخدمة بما يأتي:

(1) حفظ وتخزين سجل النظام المعلوماتي أو أي وسيلة لتقنية المعلومات لمدة مائة وثمانين يوماً متصلة. وتتمثل البيانات الواجب حفظها وتخزينها فيما يلي :

أ- البيانات التي تمكن من التعرف على مستخدم الخدمة.

ب - البيانات المتعلقة بمحتوى ومضمون النظام المعلوماتي المتعامل متى كانت تحت سيطرته.

ج - البيانات المتعلقة بحركة الاتصال

د- البيانات المتعلقة بالأجهزة الطرفية للاتصال.

هـ - أي بيانات أخرى يصدر بتحديدتها قرار من مجلس إدارة الجهاز .

Panthéon-Sorbonne (Paris I) ,IRJS, Département Sorbonne
immatériel,24 novembre 2016 14h-19h, Salle des conférences, Lycée
Henri IV, 23 rue Clovis, 75005 PARIS,p.1.

(1) **Jacques Larrieu& Christian Le Stanc& Pascale Tréfigny**:Droit du
numérique, Recueil Dalloz , N° 37 du 31/10/2013, p.2487 et s.

(2) المحافظة على سرية البيانات التي تم حفظها وتخزينها، وعدم إفشائها أو الإفصاح عنها بغير أمر مسبب من إحدى الجهات القضائية المختصة - ويشمل ذلك البيانات الشخصية لأى من مستخدمي خدمته أو أى بيانات أو معلومات متعلقة بالمواقع والحسابات الخاصة التي يدخل عليها هؤلاء المستخدمون، أو الأشخاص والجهات التي يتواصلون معها.

(3) تأمين البيانات والمعلومات بما يحافظ على سريتها، وعدم اعتراضها أو اختراقها أو تلفها.

ثانيا : مع عدم الإخلال بأحكام قانون حماية المستهلك الصادر بالقانون رقم 67 لسنة 2006، يجب على مقدم الخدمة أن يوفر لمستخدمي خدماته ولأى جهة حكومية مختصة، في الشكل، وبالطريقة التي يمكن الوصول إليها بصورة ميسرة ومباشرة ومستمرة، البيانات والمعلومات الآتية :

(1) اسم مقدم الخدمة وعنوانه.

(2) معلومات الاتصال المتعلقة بمقدم الخدمة، بما فى ذلك عنوان الاتصال الإلكتروني.

(3) بيانات الترخيص لتحديد هوية مقدم الخدمة، وتحديد الجهة المختصة التي يخضع لإشرافها.

(4) أية معلومات أخرى يقدر الجهاز أهميتها لحماية مستخدمي الخدمة، ويحددها قرار من الوزير المختص.

ثالثاً: مع مراعاة حرمة الحياة الخاصة التي يكفلها الدستور، يلتزم مقدمو الخدمة والتابعون لهم، أن يوفرُوا حال طلب جهات الأمن القومي، ووفقاً لاحتياجاتها كافة الإمكانيات الفنية التي تتيح لتلك الجهات ممارسة اختصاصاتها وفقاً للقانون.

رابعاً: يلتزم مقدمو خدمات تقنية المعلومات ووكلائهم وموزعيهم التابعون لهم المنوط بهم تسويق تلك الخدمات بالحصول على بيانات المستخدمين ويحظر على غير هؤلاء القيام بذلك.

ومن هنا يلتزم مزودو الخدمة بمجموعة من الالتزامات:

1- يجب على مزودي خدمات الاستضافة إبلاغ السلطات بعناوين هؤلاء الأشخاص، والبريد الإلكتروني والصفحة الشخصية، في حالة نشر أي بيانات أو معلومات من شأنها تهديد الأمن القومي أو الاقتصادي للدولة، أو نشر المواد الإباحية، أو التحريض على الاتجار في البشر والأعضاء البشرية، وجميع الأنشطة غير القانونية، الأمر الذي يتعين معه إلزام مزودي خدمات الاستضافة مدير تحرير الموقع بالحصول على المعلومات الشخصية للمستخدمين مسبقاً عند إنشاء صفحات التواصل الاجتماعي⁽¹⁾.

2- يلتزم مزودي خدمة الاستضافة باحترام الحق في الخصوصية، وسرية المراسلات.

(1) **Jérôme Bossan**: Le droit pénal confronté à la diversité des intermédiaires de l'internet, RSC, N° 02 du 16/08/2013, p.295.

- 3- يجب على مقدمي خدمات التقنية الرقابة على المعلومات التي تعد جريمة تهدد سلامة أمن الدولة، وإبلاغ السلطات عنها.
- 4- إذا ورد بلاغ لمقدمي الخدمات التقنية عن وجود معلومات أو بيانات غير قانونية كالتشهير بأحد الأشخاص، فيتعين عليهم الامتناع عن تخزينها.
- 5- الحفاظ على حقوق الملكية الفكرية، وعدم جواز نسخ أي بيانات أو نقلها إلى الجمهور دون موافقة أصحاب حقوق الطبع والنشر.
- 6- عدم جواز إلغاء أو حذف أو تعديل تدمير أو إفشاء أو إتلاف أو تغيير أو إعادة نشر بيانات أو معلومات.

ثالثاً: تحديد المسؤولية الجنائية لمزود الخدمة:

نص القانون رقم 175 لسنة 2018 على المسؤولية الجنائية لمقدمي الخدمة في حالة المخالفة، وذلك ما أكدته المادة (30) على أن يعاقب بالحبس مدة لا تقل عن سنة والغرامة لا تقل عن خمسمائة ألف جنيه ولا تجاوز مليون أو إحدى هاتين العقوبتين كل مقدم خدمة امتنع عن تنفيذ القرار الصادر من المحكمة الجنائية المختصة بحجب أحد المواقع أو الروابط أو المحتوى المشار إليه في الفقرة الأولى من المادة 7 من هذا القانون.

فإذا ترتب على الامتناع عن تنفيذ القرار الصادر من المحكمة وفاة شخص أو أكثر أو الأضرار بالأمن القومي وتكون العقوبة السجن المشدد وغرامه لا تقل عن ثلاثة

ملايين جنيهه ولا تجاوز عشرين مليون جنيهه، وتقضى المحكمة فضلاً عن ذلك بإلغاء ترخيص مزولة المهنة.

وبالتالي يسأل مزود الخدمة جنائياً ومدنياً عن أعمال التعدي على حقوق النشر والتأليف، وإذا كان المحتوى المتاح عبر الشبكة غير قانوني وتم سحبه من الشبكة بناءً على طلب المنتجين، ولا تتعدد المسؤولية الجنائية في حقهم عن سحب المحتوى إذا علم حقيقة بالنشاط أو المعلومات غير المشروعة، وتصرفوا بسرعة لسحب تلك المعلومات أو عدم إتاحتها، ذلك وفقاً لقرار المجلس الدستوري الفرنسي⁽¹⁾.

ويلتزم مزودو الخدمات الإلكترونية بإخطار اللجنة الوطنية المعلوماتية والحريات في حالة اختراق المعلومات والبيانات الشخصية، وذلك ما نصت عليه المادة (226-17) من قانون العقوبات الفرنسي المعدلة بموجب القرار رقم 1012-2011

(1) "Il dispose que ces personnes « ne peuvent voir leur responsabilité pénale engagée à raison des informations stockées à la demande d'un destinataire de ces services si elles n'avaient pas effectivement connaissance de l'activité ou de l'information illicites ou si, dès le moment où elles en ont eu connaissance, elles ont agi promptement pour retirer ces informations ou en rendre l'accès impossible » conseil constitutionnel, Commentaire de la décision n° 2004-496 DC du 10 juin 2004.

الصادر في 24 أغسطس 2011 بشأن الاتصالات الإلكترونية⁽¹⁾، على أن يعاقب مزودي الخدمات الإلكترونية بالسجن خمس سنوات وغرامة 300 ألف يورو إذا لم يخطر عن اختراق للبيانات الشخصية إلى اللجنة الوطنية للمعلوماتية والحريات أو صاحب الشأن، وفي مخالفة لأحكام البند ثانياً من المادة 34 مكرر من القانون رقم 17-78 الصادر في 6 يناير 1978⁽²⁾.

ويعاقب بالسجن لمدة خمس سنوات وغرامة 300 ألف يورو غرامة كل قام بإجراء معالجة إلكترونية دون مراعاة الاحتياطات اللازمة المنصوص عليها في المادة 34 من القانون رقم 17-78 الصادر في 6 يناير 1978⁽³⁾.

(1) **JORF** n°0197 du 26 août 2011 page 14473, texte n° 49, Ordonnance n° 2011-1012 du 24 août 2011 relative aux communications électroniques.

(2) **Art. 226-17-1** "(Ord. n° 2011-1012 du 24 août 2011, art. 39) Le fait pour un fournisseur de services de communications électroniques de ne pas procéder à la notification d'une violation de données à caractère personnel à la Commission nationale de l'informatique et des libertés ou à l'intéressé, en méconnaissance des dispositions du II de l'article 34 bis de la loi n° 78-17 du 6 janvier 1978, est puni de cinq ans d'emprisonnement et de 300 000 € d'amende".

(3) **Art. 226-17** "(L. n° 2004-801 du 6 août 2004, art. 14) Le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en œuvre les mesures prescrites à l'article 34 de

ويعاقب بالسجن خمس سنوات وغرامة 300 ألف يورو كل من يقوم بإهمال عند تنفيذ معالجة إلكترونية للبيانات الشخصية دون مراعاة الإجراءات اللازمة التي يجب اتباعها⁽¹⁾.

ويترتب على ما سبق أن مستخدمي الشبكة يلتزمون بضمان الحصول الآمن على المعلومات، والاستفادة من خدمات الشبكة. وفي المقابل، يقع على عاتق مزود الخدمة واجبات معينة، والتزامات.

أولاً: مع عدم الإخلال بالأحكام الواردة بقانون تنظيم الاتصالات المصري، يلتزم مقدمو خدمات الاتصالات بما يلي:

١ - حفظ وتخزين وتأمين تقنية المعلومات، ومحتوى النظم المعلوماتية، لمدة مائة وثمانون يوماً متصلة، ومحدثة بصفة مستمرة، وخاصة البيانات التي تمكن من التعرف على مستخدم الخدمة، والبيانات المتعلقة بحركة الاتصال، والبيانات المتعلقة بالأجهزة الطرفية للاتصال.

la loi no 78-17 du 6 janvier 1978 précitée est puni de cinq ans d'emprisonnement et de 300 000 € d'amende".

⁽¹⁾Art. 226-16 "(L. no 2004-801 du 6 août 2004, art. 14) Le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en œuvre prévues par la loi est puni de cinq ans d'emprisonnement et de 300 000 € d'amende".

٢ - سرية البيانات التي تم حفظها وتخزينها، وعدم الإفشاء بغير إذن أو طلب من إحدى الجهات القضائية المختصة للبيانات الشخصية لأى من مستخدمي خدمته، أو أية بيانات أو معلومات متعلقة بالمواقع أو الحسابات الخاصة التي يدخل عليها هؤلاء المستخدمون، أو الأشخاص والجهات التي يتواصلون معها.

ثانياً: مع عدم الإخلال بقانون حماية المستهلك، يجب على مقدم الخدمة أن يوفر لمستخدمي خدمته ولأى جهة حكومية مختصة، في الشكل وبالطريقة التي يمكن الوصول إليها بصورة ميسرة ومباشرة ومستمرة، البيانات والمعلومات الآتية:

١ - اسم مقدم الخدمة وعنوانه.

٢ - معلومات الاتصال المتعلقة بمقدم الخدمة، بما في ذلك عنوان الاتصال الإلكتروني.

٣ بيانات التراخيص لتحديد هوية مقدم الخدمة، وتحديد الجهة المختصة التي يخضع لإشرافها.

٤- أية معلومات أخرى يرى الجهاز أهميتها لحماية مستخدمي الخدمة، ويصدر بتحديدھا قرار من الوزير المعني بشؤون الاتصالات.

نرى ضرورة إيجاد تقنية فنية يوفرها مزود خدمات الاستضافة تسمح لمن قام بإنشاء مواقع تواصل اجتماعي بمراقبة ما يتم نشره على الموقع ورصده؛ حتى لا تُثار مشكلة شيوع الاتهام بين المدون، ومدير التحرير الذي أنشأ الصفحة التي نُشر فيها ذلك المحتوى.

يجب اتباع الإجراءات والتدابير اللازمة لضمان سلامة الأطفال ووضع قيود لقبول دخولهم إلى مواقع التواصل الاجتماعي.

يجب على مواقع التواصل الاجتماعي تبني سياسة رفع دعاوى تعويض ضد المتهمين بالتعرض لمستخدمي الشبكة الاجتماعية بالرسائل الوهمية وغير المرغوب فيها.

ويتعين تحديد شروط لاستخدام مواقع التواصل الاجتماعي؛ إذ يجب على المستخدمين استكمال تسجيلهم في هذه المواقع ببياناتهم الحقيقية، وإلزام مديري تحرير صفحات التواصل الاجتماعي بتحديد شروط مسبقاً لاستخدام هذه المواقع، تتضمن عدم استخدامها في ارتكاب جرائم.

ويجب أن يكون هناك تعاون أمني وقضائي على المستوى الدولي يتفق مع طبيعة الجرائم التي تتم عبر شبكة الإنترنت، كما يجب على الدول أن تضع أمامها قواعد لما يعد سلوكاً إجرامياً طبقاً لقواعد القانون الدولي لمحاولة التوفيق بين قواعد القانون الجنائي الدولي والداخلي، وإيجاد حماية دولية جنائية عن الجرائم التي تقع عبر مواقع التواصل الاجتماعي.

المطب الثاني

جرائم الأموال عبر مواقع التواصل الاجتماعي

تمهيد وتقسيم:

صاحب ظهور مواقع التواصل الاجتماعي تطورات كبيرة في شتى المجالات, حيث أصبحت المعاملات التجارية تتم من خلال تلك المواقع, مثل البيع والشراء, وأضحت جزء لا يتجزأ من تلك المعاملات التجارية⁽¹⁾, وفي خضم التداول المالي عبر مواقع التواصل الاجتماعي, انتهز بعض المجرمون بالاحتيال والابتزاز.

الفرع الأول: النصب عبر مواقع التواصل الاجتماعي.

الفرع الثاني: الابتزاز عبر مواقع التواصل الاجتماعي.

(1) **Khim Yong Goh & Cheng-Suang Heng & Zhijie LIN:** Social Media Brand Community and Consumer Behavior: Quantifying the Relative Impact of User- and Marketer-Generated Content, 31 October 2012, p.3 and other.

الفرع الأول

النصب عبر مواقع التواصل الاجتماعي

مع التطور وانتشار وسائل التكنولوجيا الحديثة، وخاصة مواقع التواصل الاجتماعي والتي أصبح من خلالها العالم قرية صغيرة يستطيع معها الشخص الوصول إلى ما يريد من المعلومات والأشخاص، ولم يقتصر استخدام هذه التكنولوجيا على التواصل والاتصال، بل أصبح البعض يقوم بالتجارة والتعليم لتوافر خصوصية الصوت والصورة ولم يعد يستغني عنه الكثير من الأشخاص في العالم.

ولم يعد استخدام التكنولوجيا قاصراً على المجالات النافعة، بل تعداها لتشمل المجالات الضارة التي تعود بالضرر على الأفراد وسلامة أمنهم وخصوصيتهم من سرقة ونصب وابتزاز فأصبحت الجريمة جزءاً من استخداماتها⁽¹⁾، بل أصبح هناك تطور ملموس للجريمة معها فلم تعد الجرائم قائمة على الأرض، بل تطورت بتطور التكنولوجيا حتى أنها تكاد تظهر بصورة أكثر واقعية على الأرض لظن البعض أنه لا رقابة ولا متابعة وأنه بعيد عن أعين وأيدي رجال الشرطة، فهناك العديد من الأشخاص يقعون ضحية لمخاطر اجتماعية وأخلاقية كبيرة يتسبب بها أفراد متمرسون في النصب والاحتيال والجريمة.

(1) Jean Cazeneuve: La cybercriminalité: l'émergence d'un nouveau risque, N° 05 du 14/05/2012, p.268 et s.

ويقع النصب والاحتيايل بإرسال رسالة إلى شخص على الماسنجر أو البريد الإلكتروني، يدعي فيها مرسلها أن المرسل إليه كسب ثروة، أو ميراثاً أو فاز في مسابقة، وأن البنك يحتاج إلى رسوم مصرفية يتعين دفعها، فصور الاحتيايل الإلكتروني عبر الإنترنت لا يمكن حصرها⁽¹⁾.

أولاً: النص القانوني:

نصت المادة 23 من القانون المصري رقم 175 لسنة 2018 على أن "يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر والغرامة التي لا تقل عن ثلاثين ألف جنيه ولا تجاوز خمسين ألف جنيه، أو بإحدى هاتين العقوبتين، كل من استخدم الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات، في الوصول بدون وجه حق إلى أرقام أو بيانات أو بطاقات البنوك والخدمات أو غيرها من أدوات الدفع الإلكترونية. فإن قصد من ذلك استخدامها في الحصول على أموال الغير أو ما تنتجه من خدمات، يعاقب بالحبس مدة لا تقل عن ستة أشهر وغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين.

(1) **Jacques Francillon:** Piratage informatique. Collecte de renseignements commerciaux. Délit de maintien frauduleux dans un système de traitement automatisé de données,

RSC, N° 01 du 14/03/2008, p.99.

وتكون العقوبة الحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز 200 ألف، أو إحدى هاتين العقوبتين، إذا توصل من ذلك إلى الاستيلاء لنفسه أو لغيره على تلك الخدمات أو مال الغير".

وقد جرم قانون العقوبات الفرنسي جمع البيانات والمعلومات الشخصية عن طريق الاحتيال الإلكتروني، نصت المادة 226-18 من قانون العقوبات على أن "يعاقب بالسجن خمس سنوات وغرامة كل من قام بجمع بيانات شخصية عن طريق الاحتيال أو بطريقة غير مشروعة أو غير قانونية⁽¹⁾."

وفي هذا الصدد المشرع الإماراتي تدخل في المرسوم بقانون اتحادي في شأن جرائم تقنية المعلومات رقم (5) لسنة 2012 بتجريم الأفعال التي يتم من خلالها الاستيلاء بغير حق على مال منقول أو منفعة أو على سند أو على توقيع هذا السند، وذلك بالاستعانة بأي طريقة احتيالية، أو باتخاذ اسم كاذب أو انتحال صفة غير صحيحة عن طريق الشبكة المعلوماتية، أو نظام معلومات إلكتروني أو إحدى وسائل تقنية المعلومات⁽²⁾.

ثانياً: الركن المادي:

(¹) Art. 226-18 "(L. n° 2004-801 du 6 août 2004, art. 14) Le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite est puni de cinq ans d'emprisonnement et de 300 000 € d'amende".

(²) المادة (11) من القانون رقم (5) لسنة 2012.

الاحتياى عبر مواقع التواصل الاجتماعى:

لم يعرف المشرع المصرى فى القانون رقم 175 لسنة 2018 الاحتىال الإلكترونى أو عبر مواقع التواصل الاجتماعى، على خلاف القوانين المقارنة. فقد عرف القانون الكوىى رقم (63) لسنة 2015 فى شأن مكافحة جرائم تقنية المعلومات الاحتىال الإلكترونى بأنه التأثير فى نظام إلكترونى مؤتمت أو نظام معلوماتى إلكترونى أو شبكة معلوماتية أو مستند أو سجل إلكترونى أو وثيقة تقنية معلوماتية أو نظام أو جهاز حاسب آلى أو توقيع إلكترونى أو معلومات إلكترونية ذلك عن طريق البرمجة أو الحصول أو الإفصاح أو النقل أو النشر لرقم أو كلمة أو رمز سرى أو بيانات سرية أو خاصة أخرى، بقصد الحصول على منفعة دون وجه حق أو الإضرار بالغير⁽¹⁾، ولم يعرف القانون المصرى والإماراتى الاحتىال الإلكترونى.

وعرفت الاتفاقىة العربىة لمكافحة جرائم تقنية المعلومات جريمة الاحتىال بأنه التسبب بإلحاق الضرر بالمستفدىين والمستخدمىن عن قصد وبدون وجه حق بنية الاحتىال لتحقيق المصالح والمنافع بطريقة غير مشروعة، للفاعل أو للغير، عن طريق: 1- إدخال أو تعديل أو محو أو حجب للمعلومات والبيانات؛ 2- التدخل

(1) الفقرة الأخيرة من المادة الأولى من القانون الكوىى رقم (63) لسنة 2015 فى شأن مكافحة جرائم تقنية المعلومات، صدر بقصر السىف فى 20 رمضان 1436 هـ - الموافق 7 يوليو 2015.

في وظيفة أنظمة التشغيل وأنظمة الاتصالات أو محاولة تعطيلها أو تغييرها؛ 3-
تعطيل الأجهزة والبرامج والمواقع الإلكترونية.

وللقاضي سلطة تقديرية عند تحديد الطرق الاحتمالية للحكم في جرائم الاحتيال الإلكتروني، نعتقد ضرورة النص على اعتبار الاحتيال الإلكتروني باستخدام اسم مستعار أو بطاقة مزورة أو عن طريق سرقة كلمة المرور، أو إدخال بيانات إلكترونية أو تعديل أو محو أو حجب للمعلومات والبيانات، أو سرقة هوية المستخدمين من الشبكة، أو أي تدخل في عمل نظام الكمبيوتر، أو أنظمة التشغيل والاتصالات أو البرامج أو المواقع الإلكترونية أو محاولة تعطيلها أو تغييرها، بنية احتيالية أو غير مشروعة⁽¹⁾، أو بالاستعانة بمواقع وهمية أو حقيقية للاستيلاء بغير وجه حق؛ من أجل خداع المجني عليه لحمله على تقديم أموال أو أوراق مالية أو أي ممتلكات، أو على منفعة اقتصادية أو منقول أو سند لنفسه أو للغير⁽²⁾.

انتحال الشخصية عبر مواقع التواصل الاجتماعي:

يُقصد بانتحال الشخصية الحصول بوسائل احتيالية على معلومات من الإنترنت تخص شخصاً معيناً، مثل الاسم، وتاريخ الميلاد، والمهنة، والجنسية دون علمه⁽³⁾،

(1) Cour de cassation, Chambre criminelle, 14-03-2006, n° 05-83.423.

(2) Bernard Bouloc: Collecte illicite de données nominatives, RTD Com, N° 04 du 15/12/2006, p.925.

(3) Fabrice Mattatia: L'usurpation d'identité sur internet dans tous ses états, RSC, N° 02 du 14/08/2014, p.331.

ويقع ذلك في الأغلب الأعم بهدف ارتكاب جرائم احتيال إلكتروني، أن ينتحل الجاني هوية شخص معين، ويحصل على قروض أو بطاقات ائتمان، أو يقوم بفتح حساب مصرفي⁽¹⁾.

بالرغم من نجاح مواقع التواصل الاجتماعي وتطورها، فإن مجرمي الإنترنت أحياناً يستغلون الثغرات الموجودة في نظام معلوماتي معين لاختراق هذا النظام، سواء لسرقة البيانات الشخصية للمستخدمين، أو للاطلاع على المعلومات المتوفرة في النظام ونسخها واستغلالها.

فقد أكدت المادة (24) من القانون رقم 175 لسنة 2018 على تجريم اصطناع المواقع والحسابات الخاصة والبريد الإلكتروني، حيث نصت على أن "يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر وغرامة لا تقل عن عشرة آلاف جنيه ولا تجاوز ثلاثين ألف جنيه أو بإحدى العقوبتين كل من اصطنع بريداً إلكترونياً أو موقعاً أو حاسباً خاصاً ونسبه زوراً لشخص طبيعي أو اعتباري.

فإذا استخدم الجاني البريد أو الموقع أو الحساب الخاص المصطنع في أمر يسيء إلى من نسب إليه، تكون العقوبة الحبس الذي لا تقل مدته عن سنة وغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائتي ألف جنيه، أو بإحدى العقوبتين.

وإذا وقعت الجريمة على أحد الأشخاص الاعتبارية العامة فتكون العقوبة السجن والغرامة التي لا تقل عن مائة ألف جنيه ولا تزيد على ثلاثمائة ألف جنيه".

(¹) Emilie Bailly & Emmanuel Daoud: op cit, p. p.252 et s.

وتجدر الإشارة إلى أن المشرع المصري لم يضع نصاً صريحاً يجرم سرقة الهوية وانتحال الشخصية عبر مواقع التواصل الاجتماعي، على خلاف التشريعات الأخرى التي نصت على تجريم انتحال الشخصية وسرقة الهوية عبر مواقع الإنترنت.

نصت المادة (11) من المرسوم بقانون الإماراتي رقم (5) لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات على أن "يعاقب بالحبس مدة لا تقل عن سنة واحدة والغرامة التي لا تقل عن مائتين وخمسين ألف درهم ولا تتجاوز مليون درهم أو بإحدى هاتين العقوبتين كل من استولى لنفسه أو لغيره بغير حق على مال منقول أو منفعة أو على سند أو توقيع هذا السند، وذلك بالاستعانة بأي طريقة احتيالية أو باتخاذ اسم كاذب أو انتحال صفة غير صحيحة عن طريق الشبكة المعلوماتية أو نظام معلوماتي إلكتروني أو إحدى وسائل تقنية المعلومات".

وأقرت الفقرة الخامسة من المادة (3) من القانون الكويتي رقم (63) لسنة 2015 أيضاً على أن يعاقب بالحبس مدة لا تتجاوز ثلاث سنوات وبغرامة لا تقل عن ثلاثة آلاف دينا ولا تتجاوز عشرة آلاف دينار أو بإحدى هاتين العقوبتين كل من توصل عن طريق الشبكة المعلوماتية أو باستخدام وسيلة من وسائل تقنية المعلومات إلى الاستيلاء لنفسه أو لغيره على مال أو منفعة أو مستند، وذلك باستعمال طريقة احتيالية أو باتخاذ اسم كاذب أو انتحال صفة غير صحيحة متى كان ذلك من شأنه خداع المجني عليه.

وتتم جريمة انتحال الشخصية من خلال أخذ المعلومات الشخصية الخاصة بشخص آخر دون علمه، ويلجأ القرصان الهاكر إلى ذلك بهدف الحصول على بطاقة ائتمان باسم ذلك الشخص أو عنوانه لفتح حساب مصرفي جديد، أو إنشاء الشيكات المزورة باستخدام الاسم، ورقم الحساب البنكي، والحصول على شيكات⁽¹⁾.

وقد يكون الهدف من انتحال الشخصية وسرقة الهوية عبر مواقع التواصل الاجتماعي الإضرار والمساس بسمعة الغير.

وقد أدخل القانون الفرنسي القانون رقم 267-2011 الصادر 14 مارس 2011⁽²⁾، على القانون الجنائي جريمة سرقة الهوية عبر الشبكات الرقمية والإلكترونية.

(1) **Jacques Francillon**: Piratage informatique. Usurpation d'identité numérique. L'affaire du « faux site officiel» de Rachida Dati: une étape dans la lutte contre la cyberdélinquance, RSC, N° 01 du 21/05/2015, p.101; **Yves Mayaud**: Un attendu de principe pour le délit d'usurpation d'identité, RSC, N° 01 du 12/05/2016, p.68.

(2) LOI n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure.

Cette infraction est punie des mêmes peines lorsqu'elle est commise sur un réseau de communication au public en ligne".

فقد نصت المادة (1-4-226) من قانون العقوبات على أن يعاقب بالحبس سنة وغرامة 15 ألف يورو كل من قام بانتحال صفة الغير أو استغلال بياناته الشخصية بقصد إحداث ضرر له أو مساساً بسمعته وكرامته وشرفه. ويُعاقب بذات عقوبة الجريمة إذا ارتكبت من خلال شبكة الاتصالات عبر مواقع الإنترنت⁽¹⁾.

ويعاقب على سرقة الهوية عبر مواقع التواصل الاجتماعي استناداً إلى المادة التاسعة من القانون المدني التي أكدت على احترام الحياة الخاصة. وعلى سبيل المثال، قد يقوم شخص بجمع معلومات من صفحة الفيسبوك التي تم إنشاؤها من قبل شخص آخر من الصور والتعليقات وينتحل شخصيته، ويعد ذلك اعتداءً على حياته الخاصة وانتهاكاً لحقوق صورته⁽²⁾.

وفي هذا الصدد نصت المادة (1-4-226) من قانون العقوبات على أن (القانون رقم 2011-267 الصادر 14 مارس 2011) يعاقب بالحبس سنة وغرامة 15 ألف

⁽¹⁾ **Art. 226-4-1** "(L. n° 2011-267 du 14 mars 2011, art. 2) Le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération, est puni d'un an d'emprisonnement et de 15 000 € d'amende.

Cette infraction est punie des mêmes peines lorsqu'elle est commise sur un réseau de communication au public en ligne".

⁽²⁾ **Emilie Bailly & Emmanuel Daoud**: Cybercriminalité et réseaux sociaux: la réponse pénale, AJ Pénal, N° 05 du 14/05/2012, p.252 et s.

يورو كل من قام بسرقة هوية شخص باستخدام أحد بياناته الشخصية أو أكثر بهدف إحداث ضرر له أو تعكير هدوئه أو مساساً بسمعته وكرامته وشرفه. ويُعاقب بذات العقوبة إذا ارتكبت الجريمة من خلال شبكة الاتصالات عبر مواقع الإنترنت⁽¹⁾.

يتضح لنا مما سبق أهمية تجريم انتحال الشخصية عبر مواقع التواصل الاجتماعي بنص صريح؛ لأن من شأنه أن يحمي البيانات الشخصية للمستخدم على مواقع التواصل الاجتماعي، ويحول دون استغلال هذه البيانات في ارتكاب جرائم أخرى.

لذلك يجب على المشرع المصري تعديل القانون رقم 175 لسنة 2018 بأن ينص صراحة على تجريم انتحال الشخصية على شبكة الإنترنت، ومواقع التواصل الاجتماعي، أو إحدى وسائل تقنية المعلومات.

(1) **Art. 226-4-1** "(L. n° 2011-267 du 14 mars 2011, art. 2) Le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération, est puni d'un an d'emprisonnement et de 15 000 € d'amende.

Cette infraction est punie des mêmes peines lorsqu'elle est commise sur un réseau de communication au public en ligne".

الإعلانات الوهمية عبر مواقع التواصل الاجتماعي:

تعتبر الإعلانات الوهمية سبب من أسباب ازدياد جرائم انتحال الشخصية ثم استغلالها في ارتكاب جرائم احتيال، أو تشهير وقذف، كإعلانات عبر البريد الإلكتروني غير المرغوب فيه باستغلال بوابة البنوك. وهذه المعلومات يسيء استخدامها المحتالون على شبكة الإنترنت من خلال سرقة بطاقات الائتمان وسحب أموال أصحابها من البنوك أو اصطياد الضحايا عبر الإنترنت من خلال إجراء مزاد وهمي أو عرض تأشيرات وهمية مزورة.

وقد يستغل الفيس بوك (Facebook) في التعرف إلى بيانات الأشخاص من خلال معلوماتهم وجهات الاتصال الخاصة بهم، وعناوين البريد الإلكتروني، ثم يتم إرسال العديد من رسائل البريد المزعج إليهم، وبسبب الخسائر الناجمة عن هذه الأفعال نعتقد ضرورة مراعاة المشرع المصري عند تعديل القانون النص على تجريم الإعلانات الوهمية، وكل تحايل على العنوان الإلكتروني للإنترنت باستخدام عنوان وهمي أو عنوان عائد إلى آخرين أو بأي وسيلة أخرى.

ثالثاً: العقوبة:

عاقب المشرع المصري في المادة 23 من القانون رقم 175 لسنة 2018 بالحبس مدة لا تقل عن ثلاثة أشهر والغرامة التي لا تقل عن ثلاثين ألف جنيه ولا تجاوز خمسين ألف جنيه، أو بإحدى هاتين العقوبتين، كل من استخدم الشبكة المعلوماتية

أو إحدى وسائل تقنية المعلومات، في الوصول بدون وجه حق إلى أرقام أو بيانات أو بطاقات البنوك والخدمات أو غيرها من أدوات الدفع الإلكترونية.

فإن قصد من ذلك استخدامها في الحصول على أموال الغير أو ما يتاح من خدمات، يعاقب بالحبس مدة لا تقل عن ستة أشهر وغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين.

وتكون العقوبة الحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز 200 ألف، أو إحدى هاتين العقوبتين، إذا توصل من ذلك إلى الاستيلاء لنفسه أو لغيره على تلك الخدمات أو مال الغير".

وقد عاقب قانون العقوبات الفرنسي جمع البيانات والمعلومات الشخصية عن طريق الاحتيال الإلكتروني، بمقتضى المادة 18-226 من قانون العقوبات بالسجن خمس سنوات وغرامة كل من قام بجمع بيانات شخصية عن طريق الاحتيال أو بطريقة غير مشروعة أو غير قانونية.

نعتقد أنه يجب على المشرع المصري إدراج نص في القانون رقم 175 لسنة 2018 على أن "يعاقب بالحبس مدة لا تقل عن سنتين وغرامة لا تقل عن ثلاثمائة ألف جنيه ولا تجاوز خمسمائة ألف جنيه، كل من يقوم بالإعلانات الوهمية عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات أو أحد مواقع التواصل الاجتماعي إلى الاستيلاء لنفسه أو لغيره على مال مملوك للغير أو على سند أو على أدوات إنشاء توقيع إلكتروني خاص بالغير، وكان ذلك بالاحتيال للاستيلاء على عقار مملوك للغير أو بعضه".

ويجب على مواقع التواصل الاجتماعي تبني سياسة رفع دعاوى تعويض ضد
المتهمين بالتعرض لمستخدمي مواقع التواصل الاجتماعي بالرسائل الوهمية غير
المرغوب فيها.

الفرع الثاني

الابتزاز عبر مواقع التواصل الاجتماعي

يعتبر الابتزاز⁽¹⁾ عبر مواقع التواصل الاجتماعي أحد أشكال الجريمة الإلكترونية التي أُرقت مستخدمي التكنولوجيا، وذلك لحدوث العديد من التجاوزات التي تعدت على خصوصياتهم وبياناتهم الشخصية إلى جانب صورهم وما يتعلق بحياتهم الخاصة.

فالشخص المبتز مختل اجتماعياً ولديه اضطرابات في الشخصية تجعلها يستهين بالمجتمع ومكوناته وأفراد مما يدفعه إلى البحث عن كل ما يتساق مع الضرر بهذا المجتمع كالابتزاز عبر مواقع التواصل الاجتماعي، ويعمل المبتز من خلاله المساس بأحد مكونات هذا المجتمع وهو الفرد فيقوم بالاطلاع على خصوصياته ويحاول أن يتوصل لكل ما يتعلق بالحياة الخاصة لهؤلاء المواطنين بهدف تهديدهم أو الحصول على المال أو بسبب اضطرابه ومرضه النفسي.

(1) كلمة الابتزاز مزعجة وتجلب معها قدراً كبيراً من المشاعر السلبية، فهي تجسيد لواحدة من أخطر الخصال التي يمكن أن يتحلى بها الإنسان، حين يستغل قوته مقابل ضعف إنسان آخر سواء كان هذا الضعف مؤقتاً أو دائماً، ويمر الإنسان في مراحل حياته المختلفة بتجارب من هذا النوع منذ زمن الطفولة الأولى، حين يهددك أخوك بأن يخبر أمك بأنك أنت من كسر التحفة الثمينة وأنت تلعب الكرة إن أنت لم تشركه في قالب الحلوى الذي معك، ومع التقدم في السن يصبح الابتزاز أكثر شدة على الصعيد الأسري أو العملي، فعلى الصعيد الأسري قد يبتز الزوج زوجته مقابل السماح لها بالعمل، وعلى صعيد الحياة العملية نجد أن رئيس العمل قد يبتز موظفه فيما يتعلق بالفرص التدريبية أو الترقيات ما لم يتحول.

أولاً: النص القانوني:

لم ينص القانون رقم 175 لسنة 2018 على تجريم الابتزاز عبر مواقع التواصل الاجتماعي، وكذلك قانون العقوبات⁽¹⁾ في نصوصه لم يتعرض إلى الابتزاز الإلكتروني بشكل عام، ويمكن تطبيق هذه النصوص على الابتزاز عبر مواقع التواصل الاجتماعي، وهو أن يقوم شخص بأي عمل إلكتروني لدفع شخص آخر للقيام بفعل معين مهدداً إياه في حالة عدم القيام به التشهير به أو فضحه أو نشر معلومات وبيانات خاصة بهدف الحصول على المال أو المصلحة.

أما القانون الإماراتي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات نص في المادة (16) يعاقب بالحبس مدة لا تزيد على سنتين والغرامة التي لا تقل عن مائتين وخمسون ألف درهم ولا تجاوز خمسمائة ألف درهم أو بإحدى هاتين العقوبتين كل من ابتز أو هدد شخص آخر لحمله على القيام بفعل أو الامتناع عنه وذلك باستخدام شبكة معلوماتية أو وسيلة تقنية معلومات. وتكون

(¹) نصت المادة (327) من قانون العقوبات المصري على أن كل من هدد غيره كتابة بارتكاب جريمة ضد النفس أو المال معاقب عليها بالقتل أو الأشغال الشاقة المؤبدة أو المؤقتة أو بإفشاء أمور أو نسبة أمور مخدوشة بالشرف وكان التهديد مصحوباً بطلب أو بتكليف بأمر يعاقب بالسجن. ويعاقب بالحبس إذا لم يكن التهديد مصحوباً بطلب أو بتكليف بأمر. وكل من هدد غيره شفهاياً بواسطة شخص آخر بمثل ما ذكر يعاقب بالحبس مدة لا تزيد على سنتين أو بغرامة لا تزيد على خمسمائة جنيه سواء أكان التهديد مصحوباً بتكليف بأمر أم لا. وكل تهديد سواء أكان بالكتابة أم شفهاياً بواسطة شخص آخر بارتكاب جريمة لا تبلغ الجسامة المتقدمة يعاقب عليه بالحبس مدة لا تزيد على ستة أشهر أو بغرامة لا تزيد على مائتي جنيه.

العقوبة السجن مدة لا تزيد على عشر سنوات إذا كان التهديد بارتكاب جريمة أو إسناد أمور خادشة للشرف أو الاعتبار.

كما نص المشرع الإماراتي في قانون العقوبات الاتحادي نص في المادة 378 على حماية الحياة الخاصة حيث عاقب بالحبس والغرامة "كل من اعتدى على حرمة الحياة الخاصة أو العائلية للأفراد وذلك بأن ارتكب أحد الأفعال الآتية في غير الأحوال المصرح بها قانوناً أو بغير رضاء المجني عليه:

أ- استرق السمع أو سجل أو نقل عن طريق جهاز من الأجهزة أيّاً كان نوعه محادثات جرت في مكان خاص أو عن طريق الهاتف أو أي جهاز آخر.

ب- التقط أو نقل بجهاز أيّاً كان نوعه صورة شخص في مكان خاص.

فإذا صدرت الأفعال المشار إليها في الحالتين السابقتين أثناء اجتماع على مسمع أو مرأى من الحاضرين في ذلك الاجتماع فإن رضاه هؤلاء يكون مفترضاً.

كما يعاقب بذات العقوبة من نشر بإحدى طرق العلانية أخباراً أو صوراً أو تعليقات تتصل بأسرار الحياة الخاصة أو العائلية للأفراد ولو كانت صحيحة.

نص القانون الكويتي رقم (63) لسنة 2015 في شأن مكافحة جرائم تقنية المعلومات الابتزاز الإلكتروني في الفقرة الرابعة من المادة (3) على أن يعاقب بالحبس مدة لا تجاوز ثلاث سنوات وبغرامة لا تقل عن ثلاثة آلاف دينار ولا تجاوز عشرة آلاف دينار أو بإحدى هاتين العقوبتين كل من: 1-...-2؛...-3-4؛... استعمل الشبكة المعلوماتية أو استخدم وسيلة من وسائل تقنية المعلومات

في تهديد أو ابتزاز شخص طبيعي أو اعتباري لحمله على القيام بفعل أو الامتناع عنه. فإذا كان التهديد بارتكاب جنائية أو بما يُعد مساساً بكرامة الشخص أو خادشاً للشرف والاعتبار أو السمعة كانت العقوبة الحبس مدة لا تتجاوز خمس سنوات والغرامة التي لا تقل عن خمسة آلاف دينار ولا تتجاوز عشرين ألف دينار أو بإحدى هاتين العقوبتين.

ثانياً: الركن المادي:

يعتبر الركن المادي للجريمة هو السلوك الذي يظهر إلى حيز الوجود، فهو يبرز الجريمة ويجعلها تخرج إلى العالم الخارجي.

الابتزاز هو القيام بالتهديد بكشف معلومات معينة عن شخص، أو فعل شيء لتدمير الشخص المهدد، إن لم يتم الشخص المهدد بالاستجابة إلى بعض الطلبات.

السلوك الإجرامي:

وقد عرف القانون الفرنسي (DE L'EXTORSION) الابتزاز بأنه كل فعل من شأنه التهديد بالكشف عن معلومات أو إسناد واقعة من المرجح أن تضر شرف أو سمعة، أو إفشاء سرية أمور معينة أو إتيان فعل معين، من أجل الحصول على أموال أو أوراق مالية أو أي ممتلكات⁽¹⁾.

(¹) Art. 312-1 "L'extorsion est le fait d'obtenir par violence, menace de violences ou contrainte soit une signature, un engagement ou une renonciation, soit la révélation d'un secret, soit la remise de fonds, de valeurs ou d'un bien quelconque"

وعادة ما يتم الابتزاز عبر مواقع التواصل الاجتماعي المختلفة كالفيس بوك، تويتر، وإنستجرام وغيرها من مواقع التواصل الاجتماعي، نظرًا لانتشارها الواسع واستخدامها من قبل جميع فئات المجتمع، وتتزايد عمليات الابتزاز الإلكتروني في ظل تنامي عدد مستخدمي مواقع التواصل الاجتماعي والتسارع المشهود في أعداد برامج المحادثات المختلفة.

ويمكننا تعريف الابتزاز عبر مواقع التواصل الاجتماعي بأنه القيام بتهديد وترهيب للشخص عبر مواقع التواصل الاجتماعي بنشر صور أو فيديو أو تسريب معلومات سرية تخصه، مقابل دفع مبالغ مالية أو استغلاله للقيام بأعمال غير مشروعة لصالح المبتز كالإفصاح بمعلومات سرية خاصة بجهة العمل أو غيرها من الأعمال غير القانونية.

ويتمثل الابتزاز عبر مواقع التواصل الاجتماعي محاولة الحصول على مكاسب مادية أو معنوية عن طريق الإكراه المعنوي للضحية وذلك بالتهديد بكشف أسرار أو معلومات خاصة. والابتزاز بهذه الصورة يمتد ليشمل جميع القطاعات، فنجد ما يسمى بالابتزاز السياسي والابتزاز العاطفي والابتزاز الإلكتروني، الابتزاز الإلكتروني هو الابتزاز الذي يتم باستخدام تقنية المعلومات ضد الضحايا لابتزازهم ماديا أو جنسياً.

وبهذا الصدد يعرف الابتزاز عبر مواقع التواصل الاجتماعي بأنه قيام شخص بالتعدي على خصوصية أفراد آخرين من خلال الحصول على صور أو أسرار أو

بيانات خاصة بهدف الحصول على المال، وتهديده بالكشف عن هذه المعلومات إذا لم يقم الشخص المهدد بالاستجابة إلى بعض الطلبات من المبتز.

كما يتمثل بقيام المتهم بتهديد المجنى عليها بإفشاء وفضح أمرها، بعد تحصله على مقاطع فيديو لها عن طريق التقاطه صوراً بواسطة هاتفه المحمول، وتهديدها بإفشاء أمرها ونشر الصور والمقاطع المطالبة بمبالغ مالية، فالابتزاز عبر مواقع التواصل الاجتماعي أسلوب من أساليب الإكراه، يمارسه الجاني لتحقيق مقاصده الإجرامية، وذلك للوصول إلى هدفه الذي قد يكون هدفاً مادياً أو معنوياً، وفي حال عدم استجابتها للجاني فإن الأخير سيقوم بنشر المعلومات السرية على الملأ، وهو ما يضع المجني عليها في مأزق إما بالرضوخ للجاني وتحقيق مطالبه، وإما بعدم الرضوخ والتعرض للفضيحة

بالرغم من أنه بات معروفاً لدى أغلبية مستخدمي مواقع التواصل الاجتماعي ومستخدمي الهواتف من أن البيانات الشخصية والصور يمكن سرقتها أو استدراج الضحية للحصول على صور أو فيديوهات لاستخدامها فيما بعد لابتزاز الضحية، إلا أنه حتى الآن لم تقم مصر بتشريع يمكن من خلاله حماية ضحايا الابتزاز الإلكتروني، وخاصةً عبر مواقع التواصل الاجتماعي.

النتيجة الإجرامية.

يقصد به الأثر الذي ترتب على السلوك الإجرامي للمبتز عبر مواقع التواصل الاجتماعي ضد المجني عليه، كما أنه بلغة أعم تعتبر النتيجة الإجرامية هي الاعتداء الواقع على المصلحة المعتبرة والمحمية، سواء اضر هذا الاعتداء بالمصلحة أو شكل تهديداً لها، حيث تقع النتيجة الإجرامية بمجرد قيام الجاني بتهديد المجني عليه بإفشاء سر من أسراره التي يعتبرها أمراً لا يجب الاطلاع عليه أمام المأ، وكان التهديد بأمر غير مشروع، طالما سبب ذلك الخوف والهلع والتأثير على إرادة المجني عليه بأن القى في نفسه قلقاً من قيام المبتز بتنفيذ تهديده.

علاقة السببية.

يجب أن تكون الجريمة سبباً للسلوك الإجرامي، وبدون هذه العلاقة لا يمكن نسبة الجريمة إلى الفاعل، ففي جرائم الابتزاز عبر مواقع التواصل الاجتماعي، إذا تحققت النتيجة بإفشاء أسرار المجني عليه ولكن بفعل شخص آخر لم يكن هو المبتز، أو بسبب ضياع هذه المستندات وانتشارها بمحض الصدفة، فلا مسئولية على الفاعل لانتفاء علاقة السببية، ويسأل عن جريمة أخرى وفقاً للتكييف القانوني للفعل.

ثالثاً: الركن المعنوي:

العلم: أن ينصب علم الجاني على أن ما يقوم به من الحصول على صور فاضحة لأحد الأشخاص وتهديده بهذه الصور مقابل الحصول على منفعة جريمة يعاقب

عليها قانوناً. يجب أن يكون عالماً بماهية الفعل أو الامتناع المجرم، كما يعلم أن فعله يلحق ضرراً بالمجني عليه، فهذه الجريمة لا تكون إلا عمدية.

الإرادة:-

يجب أن تتجه إرادة الجاني للسلوك والنتيجة في نفس الوقت، كمن يعقد عزمه بأن يقوم بابتزاز فتاة عبر مواقع التواصل الاجتماعي بمعلومات سرية تشينها، وإرادة تحقق نتيجة أن يحصل على المال.

رابعاً: عقوبة الابتزاز عبر مواقع التواصل الاجتماعي:

لم يتطرق القانون رقم 175 لسنة 2018 على تجريم الابتزاز عبر مواقع التواصل الاجتماعي، وهو أن يقوم شخص بأي عمل إلكتروني لدفع شخص آخر للقيام بفعل معين مهدداً إياه في حالة عدم القيام به التشهير به أو فضحه أو نشر معلومات وبيانات خاصة بهدف الحصول على المال أو المصلحة.

أما القانون الإماراتي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات نص عقوبة الحبس مدة لا تزيد على سنتين والغرامة التي لا تقل عن مائتين وخمسون ألف درهم ولا تجاوز خمسمائة ألف درهم أو بإحدى هاتين العقوبتين كل من ابتز أو هدد شخص آخر لحمله على القيام بفعل أو الامتناع عنه وذلك باستخدام شبكة معلوماتية أو وسيلة تقنية معلومات. وتكون العقوبة السجن مدة لا تزيد على عشر سنوات إذا كان التهديد بارتكاب جنائية أو إسناد أمور خادشة للشرف أو الاعتبار.

وجاء القانون الإماراتي لحماية اشمل لمستخدمي الإنترنت, وذلك بالنص على الحماية صراحة ضد كل من استعمل الإنترنت أو إحدى وسائل تقنية المعلومات في ابتزاز أو تهديد أي شخص.

وعاقب القانون الكويتي رقم (63) لسنة 2015 في شأن مكافحة جرائم تقنية المعلومات الابتزاز الإلكتروني بالحبس مدة لا تجاوز ثلاث سنوات وبغرامة لا تقل عن ثلاثة آلاف دينار ولا تجاوز عشرة آلاف دينار أو بإحدى هاتين العقوبتين كل من استعمل الشبكة المعلوماتية أو استخدم وسيلة من وسائل تقنية المعلومات في تهديد أو ابتزاز شخص طبيعي أو اعتباري لحمله على القيام بفعل أو الامتناع عنه. فإذا كان التهديد بارتكاب جريمة أو بما يُعد مساساً بكرامة الشخص أو خادشاً للشرف والاعتبار أو السمعة كانت العقوبة الحبس مدة لا تجاوز خمس سنوات والغرامة التي لا تقل عن خمسة آلاف دينار ولا تجاوز عشرين ألف دينار أو بإحدى هاتين العقوبتين.

يتبين لنا مما سبق أن المشرع المصري لم يشر في القانون رقم 15 لسنة 2018 إلى جريمة الابتزاز عبر مواقع التواصل الاجتماعي باستخدام المعلومات الشخصية للضحية، ونص القانون على أنه يُعاقب بالحبس مدة لا تقل عن سنتين، وغرامة لا تقل عن عشرين ألف جنيه، ولا تجاوز مائة ألف جنيه، كل من حاز أو أحرز أو صنع أو صدر أو تداول صورة من صور التداول عبر الإنترنت.

فتلك المادة تُعاقب فقط على استخدام البيانات أو تسهيل ارتكاب جريمة من الجرائم عبر مواقع الإنترنت، إلا أنها لا تعاقب على انتهاك خصوصية المستخدم أو استخدام بياناته، ولا تحمي البيانات الشخصية، وتداول الصور، وتركيبها على صور أخرى.

وبالنظر إلى القانون الإماراتي لمكافحة جرائم تقنية المعلومات، نجد أن المشرع نص على العقوبة، آخذاً في ذلك جانب صياغة التشديد، ونجد أنه عاقب حالات الابتزاز والتهديد، لإجبار شخص على القيام بفعل ضد إرادته، إلا أنه لم يذكر إن كانت العقوبة تسري على الفعل سواء كان مشروعاً أم غير مشروع، باستخدام مواقع التواصل الاجتماعي أو وسيلة تقنية معلومات، ونعتقد أن المشرع الإماراتي قد جعل العقوبة الأصلية الحبس والغرامة مجتمعين، وحدد الحبس في حده الأعلى بسنتين، وكذلك حدد الغرامة في حدها الأعلى خمسمائة ألف درهم، ولم يضع حداً أدنى للحبس والغرامة، تاركاً ذلك الحد الأدنى للقواعد العامة، كما أنه ترك للقاضي سلطة التقدير في الجمع بين الحبس والغرامة أو اختيار أحدهما حسبما يترأى له من ظروف القضية، ومن ظروف الجاني، ونوع الابتزاز، وطريقته، والضرر من ترويع المجني عليه، وانتشار الأسرار من عدمه، ونرى أنه جعل الحد الأعلى للحبس سنتين مشدداً بذلك مدة الحبس، إلا أننا نرى أن المشرع الإماراتي قد أحسن صنفاً في تشديد العقوبة، وذلك لجعل العقوبة السجن يصل إلى عشر سنوات إذا كان التهديد بارتكاب جناية أو بإسناد أمور خادشه للشرف والاعتبار، إلا أنه لم يتبين من التشديد إن كان يقع منفرداً أم يمكن جمعه مع الغرامة في حدها الأعلى

خمسمائة ألف درهم، وبهذا يضع المشرع الإماراتي ردعاً قوياً حين يتصل التهديد بارتكاب جنائية، أو يكون التهديد له علاقة بإسناد أمور تمس الشرف والاعتبار، ونتمنى على المشرع المصري أن يحذو حذو المشرع الإماراتي في تشديد العقوبة. نعتقد أن الابتزاز عبر مواقع التواصل الاجتماعي هو دخول مشروع أو غير مشروع عبر إحدى مواقع التواصل الاجتماعي لشخص ما لتهديده أو ابتزازه، لحمله على القيام بفعل معين أو الامتناع عنه، فالابتزاز يعد جريمة أخلاقية قبل أن يكون جريمة معاقب عليها قانونياً.

وأحياناً يكون ضحايا الابتزاز عبر مواقع التواصل الاجتماعي أطفال، لذلك نرى ضرورة إنشاء قسم لتلقي بلاغات التحرش الافتراضي والتغريب بالأطفال عبر الإنترنت، إذ يمكن استغلال مواقع التواصل الاجتماعي في استدراج الأطفال، وابتزازهم، باستغلال ضعف الإدراك لديهم، ما يجعل ابتزازهم والتغريب بهم سهلاً؛ لأن أجهزة الاتصال بالإنترنت تقدم بيئة خصبة للجرائم الموجهة ضد الأطفال بسبب صعوبة وقوعها تحت رقابة الأسرة.

كما يجب التوعية بخطر الابتزاز عبر مواقع التواصل الاجتماعي وخاصة المدارس لإعطاء محاضرات توعية لطلاب الجامعات والمدارس حول خطر الابتزاز.

نعتقد أن المشرع المصري جانبه الصواب لعدم نصه على عقوبة الابتزاز عبر مواقع التواصل الاجتماعي، لذا نقترح على المشرع إضافة نص في قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018 على أن "يعاقب بالسجن مدة لا تقل

عن ثلاث سنوات وبغرامة لا تقل عن خمسين ألف ولا تزيد على مائة وخمسين ألف جنيه كل من استخدم موقع إلكتروني أو موقعاً للتواصل الاجتماعي أو وسيلة من وسائل تقنية المعلومات في تهديد أو ابتزاز شخص طبيعي أو اعتباري لحمله على القيام بفعل أو الامتناع عنه. وإذا كان التهديد بارتكاب جناية أو يعد مساساً بالكرامة الإنسانية أو خادشاً للشرف والاعتبار والسمعة كانت العقوبة السجن وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز مائتين ألف جنيه، وتُشدّد العقوبة في حالة وقوع الجريمة على طفل أو عديم الأهلية".

المطلب الثالث

الإرهاب عبر مواقع التواصل الاجتماعي

أصبح الإرهاب ظاهرة خطيرة تهدد المجتمع في جميع أنحاء العالم، ويظهر ذلك من خلال التزايد الكبير في العمليات الإرهابية وتنوع صورها واتخاذها أشكالاً متعددة وامتدادها إلى مختلف بلدان العالم، رغم توجهاتها السياسية أو الإيديولوجية، لما تمتاز به هذه الجريمة من آثار مدمرة ضد الإنسانية، حيث اتخذت هذه الجريمة العديد من الأشكال والأساليب المستحدثة والتي يصعب ضبطها والسيطرة عليها.

وقد ظهر الإرهاب عبر مواقع التواصل الاجتماعي، وهو سلوك غير قانوني يتم باستخدام الأجهزة الإلكترونية وتقنية المعلومات، الذي ينتج عنه التهديد بالقيام بأعمال عنف موجهة ضد المجتمع أو لتسهيل القيام بأعمال إرهابية أو دعم جماعة أو تنظيم أو جمعية تقوم بأعمال إرهابية، أو الترويج لاتباع أفكارها أو تمويلها.

وتلك الجرائم قد تهدد أمن الدولة وسلامتها، وقد بذلت جمهورية مصر العربية جهوداً مضنية بهدف الوصول إلى الآليات المناسبة التي تحد من العمليات الإرهابية التي يتم تدبيرها عبر مواقع التواصل الاجتماعي كخطوة رئيسية في وضع عقوبة لها تكون رادعة.

الفرع الأول

مفهوم الإرهاب عبر مواقع التواصل الاجتماعي

يقوم الإرهابيون بإنشاء مواقع لهم عبر مواقع التواصل الاجتماعي لنشر فكرهم ودعوتهم إلى المبادئ التي يؤمنون بها، وكذلك الوسائل التي يتبعونها للقيام بالعمليات الإرهابية، وكيفية الدخول إلى المواقع واختراقها وتدميرها، وكذلك بهدف تجنيد أشخاص جدد إلى الجماعة أو التنظيم الإرهابي. ومما يزيد من خطورة المواقع عبر الإنترنت هو أن الجماعات الإرهابية تعتمد في خططها على طرق بسيطة تتيح للجميع الدخول إلى مواقع محجوبة عبر التصفح العادي أو عبر البرامج التبادلية.

كما أن الإرهابيين يستخدمون المواقع لنشر معلومات حول آلية إعداد المتفجرات والمواد السامة وصناعة الصواعق بشكل يمكن الآخرين من الحصول على الكثير منها من أي مكان دون إثارة الريبة.

أولاً: تعريف الإرهاب عبر مواقع التواصل الاجتماعي:

عرف القانون المصري رقم (94) لسنة 2015 بشأن قانون مكافحة الإرهاب في المادة الثانية، العمل الإرهابي بأنه كل استخدام للقوة أو العنف أو التهديد أو الترويع في الداخل أو الخارج، بغرض الإخلال بالنظام العام أو تعريض سلامة المجتمع أو مصالحه أو أمنه للخطر، أو إيذاء الأفراد أو إلقاء الرعب بينهم، أو تعريض حياتهم أو حرياتهم أو حقوقهم العامة أو الخاصة أو أمنهم للخطر، أو غيرها من الحريات

والحقوق التي كفلها الدستور والقانون، أو الإضرار بالوحدة الوطنية أو السلام الاجتماعي أو الأمن القومي، أو إلحاق الضرر بالبيئة أو بالموارد الطبيعية أو بالآثار أو بالأموال أو بالمباني أو بالأماكن العامة أو الخاصة، أو احتلالها أو الاستيلاء عليها، أو منع أو عرقلة السلطات العامة أو الجهات أو الهيئات القضائية أو مصالح الحكومة أو الوحدات المحلية أو دور العبادة أو المستشفيات أو مؤسسات ومعاهد العلم أو البعثات الدبلوماسية والقنصلية، أو المنظمات والهيئات الإقليمية والدولية في مصر من القيام بعملها أو ممارستها لكل أو بعض أوجه نشاطها أو مقاومتها، أو تعطيل تطبيق أي من أحكام الدستور أو القوانين أو اللوائح.

وكذلك كل سلوك يرتكب بقصد تحقيق أحد الأغراض المبينة بالفقرة الأولى من هذه المادة، أو الإعداد لها أو التحريض عليها، إذا كان من شأنه الإضرار بالاتصالات أو بالنظم المعلوماتية أو بالنظم المالية أو البنكية، أو بالاقتصاد الوطني أو بمخزون الطاقة أو بالمخزون الأمني من السلع والمواد الغذائية والمياه، أو بسلامتها أو بالخدمات الطبية في الكوارث والأزمات.

لقد توسع المشرع المصري في تعريف الجريمة الإرهابية وحاول في هذا التعريف إضافة صور أخرى للتجريم، ولقد نجح المشرع من خلال تعريفه للعمل الإرهابي بالجمع بين التأثير النفسي والمعنوي وهو إدخال الرعب والخوف والتأثير المادي الناتج من العمل الإرهابي، إلا أنه لم يذكر صراحة الإرهاب والتنظيم الإرهابي عبر مواقع التواصل الاجتماعي باعتباره صورة من صور الإرهاب.

وقد عرف المشرع الفرنسي (actes de terrorisme) الأعمال الإرهابية, بموجب المادة (1-421) من قانون العقوبات⁽¹⁾, يعد عملاً إرهابياً قيام أي شخص أو

(1) **Art. 421-1** "Constituent des actes de terrorisme, lorsqu'elles sont (L. n° 96-647 du 22 juill. 1996) «intentionnellement» en relation avec une entreprise individuelle ou collective ayant pour but de troubler gravement l'ordre public par l'intimidation ou la terreur, les infractions suivantes:

1° Les atteintes volontaires à la vie, les atteintes volontaires à l'intégrité de la personne, l'enlèvement et la séquestration ainsi que le détournement d'aéronef, de navire ou de tout autre moyen de transport, définis par le livre II du présent code;

2° Les vols, les extorsions, les destructions, dégradations et détériorations, ainsi que les infractions en matière informatique définis par le livre III du présent code;

(L. n° 96-647 du 22 juill. 1996) «3° Les infractions en matière de groupes de combat et de mouvements dissous définies par les articles 431-13 à 431-17 et les infractions définies par les articles 434-6 et 441-2 à 441-5;»

(Ord. n° 2012-351 du 12 mars 2012, art. 8, en vigueur le 1^{er} mai 2012) «4° Les infractions en matière d'armes, de produits explosifs ou de matières nucléaires définies par (L. n° 2014-1353 du 13 nov. 2014, art. 4) «les (L. n° 2016-731 du 3 juin 2016, art. 26) «articles 222-52 à 222-54, 322-6-1 et 322-11-1» du présent code,» le I de l'article L. 1333-9, les articles L. 1333-11 et L. 1333-13-2, le II des articles L. 1333-13-3 et L. 1333-13-4, les articles L. 1333-13-6, L. 2339-2, L. 2339-14, L. 2339-16, L. 2341-1, L. 2341-4, L. 2341-5, L. 2342-57

تنظيم جماعي (القانون رقم 96-647 الصادر 22 يوليو 1996)⁽¹⁾ عمداً بهدف
إحداث اضطراب خطير بالنظام العام عن طريق التهريب أو الترويع , بارتكاب
الجرائم التالية:

à L. 2342-62, L. 2353-4, le 1^o de l'article L. 2353-5 et l'article L. 2353-13 du code de la défense, ainsi que les articles (Abrogé par L. n^o 2016-731 du 3 juin 2016, art. 26) «L. 317-4,» L. 317-7 et L. 317-8 à l'exception des (L. n^o 2012-304 du 6 mars 2012, art. 33 et 34-XVI, en vigueur le 6 sept. 2013) «armes de la catégorie D définies par décret en Conseil d'État [ancienne rédaction: armes de la 6^e catégorie]», du code de la sécurité intérieure»; — V. Décr. n^o 2014-289 du 4 mars 2014 portant publication de la convention internationale pour la répression des actes de terrorisme nucléaire, signée à New-York le 14 sept. 2005 (JO 6 mars).

(L. n^o 96-647 du 22 juill. 1996) «5^o Le recel du produit de l'une des infractions prévues aux 1^o à 4^o ci-dessus»;

(L. n^o 2001-1062 du 15 nov. 2001, art. 33; L. n^o 2003-239 du 18 mars 2003, art. 31) «6^o Les infractions de blanchiment prévues au chapitre IV du titre II du livre III du présent code;

«7^o Les délits d'initié prévus (L. n^o 2016-819 du 21 juin 2016, art. 1^{er}, en vigueur le 3 juill. 2016) «aux articles L. 465-1 à L. 465-3» du code monétaire et financier.»".

(¹) JORF n^o170 du 23 juillet 1996 page 11104, LOI no 96-647 du 22 juillet 1996 tendant à renforcer la répression du terrorisme et des atteintes aux personnes dépositaires de l'autorité publique ou chargées

- 1- الاعتداء العمدي على حياة وسلامة الإنسان والاحتجاز وخطف الطائرات والسفن أو أية وسيلة نقل أخرى.
- 2- السرقة والابتزاز والتدمير والإتلاف والضرر، بالإضافة إلى الجرائم المرتكبة في مجال تقنية المعلومات، كما هي محددة في الكتاب الثالث من قانون العقوبات.
- 3- الجرائم المتعلقة بالجماعات المسلحة والحركات السياسية المنصوص عليها في المواد 13-431 حتى 17-431 والجرائم المنصوص عليها في المواد 2-441, 6-434 حتى 5-441.
- 4- (القرار رقم 2012-351 الصادر 12 مارس 2012)⁽¹⁾ تصنيع أو حيازة أدوات قاتلة أو المتفجرات بالإضافة إلى الأسلحة الكيماوية والنوية والبيولوجية المحددة في (القانون رقم 2014-1353 الصادر 13 نوفمبر 2014)⁽²⁾,

d'une mission de service public et comportant des dispositions relatives à la police judiciaire.

⁽¹⁾ **JORF** n°0062 du 13 mars 2012 page 4533, texte n° 16, Ordonnance n° 2012-351 du 12 mars 2012 relative à la partie législative du code de la sécurité intérieure.

⁽²⁾ **JORF** n°0263 du 14 novembre 2014 page 19162, texte n° 5, LOI n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme .

و(القانون رقم 2016-731 الصادر 3 يونيو 2016)¹ "المواد 222-52 إلى 222-54، 322-6-1، 322-11-1 من هذا القانون، وبعض من مواد قانون الدفاع.

- 5- إخفاء ما ينتج عن الجرائم المذكور في الفقرات السالفة الذكر.
- 6- (القانون رقم 2001-1062 الصادر 15 نوفمبر 2001)، (القانون رقم 2003-239 الصادر 18 مارس 2003) جرائم غسل الأموال المنصوص عليها في الفصل الرابع من الباب الثاني من الكتاب الثالث من هذا القانون. وعرفت الاتفاقية العربية لمكافحة الإرهاب في الفقرة الثانية من المادة الأولى الإرهاب بأنه: "كل فعل من أفعال العنف أو التهديد به أياً كانت بواعثه أو أغراضه، يقع تنفيذاً لمشروع إجرامي فردي أو جماعي، ويهدف إلى إلقاء الرعب بين الناس، أو ترويعهم بإيذائهم أو تعريض حياتهم أو حريتهم أو أمنهم للخطر، أو إلحاق الضرر بالبيئة أو بأحد المرافق أو الأملاك العامة أو الخاصة، أو احتلالها أو الاستيلاء عليها، أو تعريض أحد الموارد الوطنية للخطر".

أدى ظهور الإنترنت إلى تغييرات عديدة في العالم، وأصبح الاعتماد على وسائل تقنية المعلومات الحديثة يزداد يوماً بعد يوم، سواء في المؤسسات المالية، أو

(¹) JORF n°0129 du 4 juin 2016, texte n° 1, LOI n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale.

المرافق العامة، أو المجال التعليمي، أو الأمني أو غير ذلك، وإن للوسائل الإلكترونية الحديثة ما يصعب حصرها من فوائد، فإن الوجه الآخر والمتمثل في الاستخدامات السيئة والضارة لهذه التقنيات الحديثة ومنها الإرهاب عبر مواقع التواصل الاجتماعي أصبح خطر يهدد العالم بأسره، إن خطر الإرهاب عبر مواقع التواصل الاجتماعي يكمن في سهولة استخدام هذا السلاح مع شدة أثره وضرره، فيقوم مستخدمه بالتنظيم الإرهابي وهو في منزله، أو مكتبه، أو في مقهى، أو حتى من غرفته في أحد الفنادق.

ويعتمد الإرهاب عبر مواقع التواصل الاجتماعي على استخدام الإمكانيات العلمية والتقنية، واستغلال وسائل الاتصال والشبكات المعلوماتية، من أجل تنظيم شبكات إرهابية أو تخويف وترويع الآخرين، وإلحاق الضرر بهم، أو تهديدهم.

نعتقد أنه لا سبيل إلى مكافحة التنظيم الإرهابي عبر مواقع التواصل الاجتماعي، إلا باستخدام الأساليب العلمية الحديثة، وهي التي تؤدي إلى كشف الأدلة العلمية التي توجد الصلة بين الإرهابي وجريمته. فكل من يتعامل مع مسرح الحادث الإرهابي ينبغي أن يكون ملماً بتلك

يكمن دور الأساليب العلمية الحديثة في تحديد مرتكبي التفجيرات الإرهابية ومتطلبات تطبيقها؛ لأن الاعتماد على الطرق التقليدية في إدارة مسرح الحادث الإرهابي والتعامل مع آثاره.

ثانياً: خصائص الإرهاب عبر مواقع التواصل الاجتماعي:

الإرهاب والتنظيم الإرهابي عبر مواقع التواصل الاجتماعي له عدة خصائص وهي:

1- ترتكب الجريمة في بيئة رقمية ولذلك فإن الجاني بحاجة إلى استخدام الحاسب الآلي ليصل إلى مسرح الجريمة.

2- تتسم بالخطورة البالغة حيث تؤدي إلى إحداث خسائر كبيرة وإلى تهديد الدول وتهديد أمنها القومي، ونشر الخوف بين المواطنين وترويعهم، والإخلال بالنظام العام، تهديد السلطات والاعتداء عليها، تدمير الأمن العام، إسقاط الأنظمة.

3- صعوبة اكتشاف الإرهابيين، حيث يمكنهم ارتكاب أنشطتهم الإجرامية عن بعد عبر مواقع التواصل الاجتماعي، فيتحقق لهم ما يريدون، ذلك لأن هؤلاء لديهم خبرة عالية بتكنولوجيا المعلومات، ويمكنهم توظيف موقع التواصل الاجتماعي واستغلاله دون أن يكون بمقدور الأجهزة الأمنية الوصول إليهم.

4- سهولة التواصل بين الإرهابيين من خلال مواقع التواصل الاجتماعي أو الرسائل الإلكترونية أو الجروب أو غيره، وذلك من شأنه أن يصعب تحديد أماكنهم.

5- الإرهاب عبر مواقع التواصل الاجتماعي يتسم بكونه ينتمي إلى طائفة الجريمة المنظمة أو يشترك في بعض خصائصها.

6- يعتبر الإرهاب عبر مواقع التواصل الاجتماعي جريمة عابرة للحدود، فقد يقع السلوك الإجرامي في مكان والنتيجة الإجرامية في مكان آخر.

7- يعتبر الدليل الرقمي هو الدليل الوحيد للإثبات في هذا النوع من الجرائم، وهذا الدليل عرضة للتخريب بسهولة.

الفرع الثاني

تجريم الإرهاب عبر مواقع التواصل الاجتماعي

تعمل الجماعات الإرهابية على استغلال ثورة تكنولوجيا المعلومات في ترويج أفكارها ومحاولة غسل عقول الشباب وتجنيدهم باسم الدين، وخاصة أن السيطرة على الفضاء الرقمي لم تعد ممكنة في ظل التكنولوجيا الإعلامية الحديثة، وأصبح من الصعب ملاحقة أو مراقبة هذا الكم الكبير من وسائل الإعلام ومواقع التواصل الاجتماعي التي تروج للفكر الإرهابي وتدعو إليه، فلا بد من تجريم تلك الأفعال.

النص القانوني:

نصت المادة (12) من قانون مكافحة الإرهاب المصري رقم (94) لسنة 2015 على أن "يعاقب بالإعدام أو السجن المؤبد كل من أنشأ أو أسس أو نظم أو أدار جماعة إرهابية أو تولى زعامة أو قيادة فيها. ويعاقب بالسجن المشدد كل من انضم إلى جماعة إرهابية أو شارك فيها بأية صورة مع علمه بأغراضها وتكون العقوبة السجن المشدد الذي لا تقل مدته عن عشر سنوات إذا تلقى الجاني تدريبات عسكرية أو أمنية أو تقنية لدى الجماعة الإرهابية لتحقيق أغراضها أو كان الجاني من أفراد القوات المسلحة أو الشرطة. ويعاقب بالسجن المؤبد كل من أكره شخصا على الانضمام إلى الجماعة الإرهابية أو منعه من الانفصال عنها. وتكون العقوبة الإعدام إذا ترتب على الإكراه أو المنع وفاته".

أولاً: أركان جريمة الإرهاب عبر مواقع التواصل الاجتماعي:

تعد جريمة الإرهاب عبر مواقع التواصل الاجتماعي من أخطر الجرائم، وخطورة الإرهاب لا تقاس بعدد الضحايا الذين يسقطون على مسرح العمليات الإرهابية أو بعدد مرتكبيه، وإنما يقاس بقدرة الإرهاب على نشر الخطر، فكل انفجار مروع جديد في أي مكان في العالم يولد شعوراً بالخوف والفرع ليس على مستوى البلد الذي وقع فيه فحسب وإنما على مستوى العالم كله ذلك أن الإرهاب غير محدد بمناطق جغرافية معينة، وأشخاص بذاتهم.

الركن المادي:

وتتمثل صور الركن المادي لجريمة الإرهاب عبر مواقع التواصل الاجتماعي:

1- استخدام مواقع التواصل الاجتماعي أو أي وسيلة نشر أو إعلان إلكترونية لتسهيل القيام بأعمال إرهابية أو لدعم جماعة أو تنظيم أو جمعية تقوم بأعمال إرهابية، كأن يقوم الجاني باستخدام الشبكة المعلوماتية أو النظام المعلوماتي لتجنيد أشخاص للقيام بتنفيذ عمليات إرهابية أو لجمع معلومات أو للتحضير لهجمات مادية.

2- إنشاء موقع على فيس بوك أو تويتر أو غيره لتسهيل القيام بأعمال إرهابية أو لدعم جماعة أو تنظيم أو جمعية تقوم بأعمال إرهابية، فالهدف الأساسي من إنشاء الموقع الإلكتروني هو تسهيل القيام بأعمال إرهابية، كأن يقوم الجاني

بنشر مواد تدريبية على الأعمال الإرهابية أو على صناعة المواد المتفجرة، أو لتبادل المعلومات بين أفراد الجماعة أو التنظيم.

3- الترويج لأفكار جماعة أو تنظيم أو جمعية تقوم بأعمال إرهابية من خلال مواقع التواصل الاجتماعي أو الموقع الإلكتروني والدعوة لنشر هذه الأفكار واعتناقها وحث الأفراد على اتباعها.

4- استخدام مواقع التواصل الاجتماعي أو المواقع الإلكترونية لتمويل الجماعة أو التنظيم أو الجمعية التي تقوم بأعمال إرهابية، فالهدف هنا هو استغلال النظام المعلوماتي أو الشبكة المعلوماتية من أجل الحصول على التمويل المادي والتبرعات المالية.

5- استخدام مواقع التواصل الاجتماعي أو الموقع الإلكتروني بأي عمل من شأنه تعريض المواطنين وممتلكاتهم للخطر، كنشر الفتن الطائفية والكراهية والعنف والاعتداء على الأديان والمعتقدات بواسطة الفيس بوك أو تويتر أو المواقع الإلكترونية الأخرى.

الركن المعنوي:

جريمة الإرهاب والتنظيم الإرهابي عبر مواقع التواصل الاجتماعي جريمة عمدية، يلزم لتحقيق ركنها المعنوي توافر القصد العام، يقتصر على العلم والإرادة، ويتحقق العلم بإحاطة الجاني بعناصر الركن المادي للجريمة، الفعل والنتيجة وعلاقة السببية، وتتحقق الإرادة، باتجاه إرادة الجاني إلى إتيان عناصر الركن المادي للجريمة.

وتوافر القصد الخاص إلى جانب القصد العام، فلا بد أن تتجه إرادة الجاني عند قيامه بنشاطه الإرهابي إلى تحقيق غاية معينة، وهي تعريض سلامة المجتمع وأمنه للخطر والإخلال بالنظام العام⁽¹⁾، ذلك أن معنى الإرهاب كما ورد في القانون رقم (94) لسنة 2015 يتضمن شرطين أساسيين، الأول: استخدام العنف أو التهديد باستخدامه، الثاني أن يكون هناك قصد خاص وغاية أبعد، وهي إلقاء الرعب بين الناس وترويعهم وتعريض حياتهم أو حرياتهم أو حقوقهم العامة لخطر، فليس مجرد استخدام الجاني للعنف يعتبر إرهاباً، إنما كل ترويع للمجتمع والإخلال بالأمن في الداخل والخارج.

وأن يكون الجاني قد استهدف بفعله وهو يقوم باستخدام مواقع التواصل الاجتماعي أو الموقع الإلكتروني لتسهيل القيام بأعمال إرهابية أو دعم جماعة أو تنظيم أو جمعية تقوم بأعمال إرهابية أو الترويج لأفكارها أو تمويلها بهدف تعريض سلامة المجتمع وأمنه للخطر والإخلال بالنظام العام وإلقاء الرعب بين الناس وترويعهم.

ثانياً: عقوبة جريمة الإرهاب عبر مواقع التواصل الاجتماعي:

أقرت المادة (12) من قانون مكافحة الإرهاب المصري رقم (94) لسنة 2015 على عقوبة الإعدام أو السجن المؤبد كل من أنشأ أو أسس أو نظم أو أدار

(¹) **Bertrand de Lamy**: La lutte contre le terrorisme à l'épreuve du contrôle de constitutionnalité: utiles précisions sur la nécessité d'une incrimination, RSC, N° 02 du 11/08/2017, p.385.

جماعة إرهابية أو تولى زعامة أو قيادة فيها. والسجن المشدد لأي شخص انضم إلى جماعة إرهابية أو شارك فيها بأية صورة مع علمه بأغراضها وتكون العقوبة السجن المشدد الذي لا تقل مدته عن عشر سنوات إذا تلقى الجاني تدريبات عسكرية أو أمنية أو تقنية لدى الجماعة الإرهابية لتحقيق أغراضها أو كان الجاني من أفراد القوات المسلحة أو الشرطة. وبالسجن المؤبد كل من أكره شخصاً على الانضمام إلى الجماعة الإرهابية أو منعه من الانفصال عنها. وتكون العقوبة الإعدام إذا ترتب على الإكراه أو المنع وفاته.

يتبين أن المشرع المصري لم ينص صراحة على تجريم الإرهاب عبر مواقع التواصل الاجتماعي؛ ولكنه جرم الانضمام إلى جماعة إرهابية أو شارك فيها بأية صورة، بما فيها عن طريق مواقع التواصل الاجتماعي مع علمه بأغراضها، وجعل عقوبة السجن المشدد الذي لا يقل عن عشر سنوات إذا تلقى تدريبات تقنية أو أمنية عسكرية لدى الجماعة الإرهابية لتحقيق أغراضها عن طريق مواقع التواصل الاجتماعي، كما عاقب كل من أكره شخصاً مادياً أو معنوياً على الانضمام إلى الجماعة الإرهابية أو منعه من الانفصال عنها، وإذا ترتب على الإكراه أو المنع وفاته تصبح العقوبة الإعدام.

وجاء القانون رقم 175 لسنة 2018 ونص في المادة (34) على أن إذا وقعت أي جريمة من الجرائم المنصوص عليها في هذا القانون بغرض الإخلال بالنظام العام أو تعريض سلامة المجتمع وأمنه للخطر، أو الإضرار بالأمن القومي للبلاد

أو بمركزها الاقتصادي أو منع أو عرقلة ممارسة السلطات العامة لأعمالها، أو تعطيل أحكام الدستور أو القوانين أو اللوائح أو الإضرار بالوحدة الوطنية والسلام الاجتماعي تكون العقوبة السجن المشدد.

نعتقد أن المشرع المصري جانبه الصواب، حيث إنه لم ينص صراحة على عقاب القيام أو الإكراه أو التحريض على الانضمام لجماعة إرهابية عن طريق مواقع التواصل الاجتماعي.

ونص المشرع الفرنسي صراحة على عقاب استخدام مواقع الإلكترونيّة لأغراض الأعمال الإرهابية، حيث صدر القانون رقم 258-2017 في 28 فبراير 2017 بشأن الأمن العام⁽¹⁾، نصت المادة (421-2-5) من قانون العقوبات على أن يعاقب بالحبس عامين وغرامة قدرها 30 ألف يورو كل من قام بعمل إرهابي عن طريق الاستخدام غير المشروع لخدمات الاتصال عبر الإنترنت من خلال توفير الرسائل والصور بهدف ارتكاب أعمال إرهابية أو التحريض على القيام بهذه الأفعال، وتتضمن هذه الخدمة بنشر صور أو بيانات تبين ارتكاب أعمال العنف والاعتداء على الحياة، مع توافر مظاهر تفيد التمسك أيديولوجية على هذه الخدمة.

(¹) JORF n°0051 du 1 mars 2017, texte n° 3, LOI n° 2017-258 du 28 février 2017 relative à la sécurité publique.

وخاصاً إذا كان السبب مشروعاً على النحو المحدد في الفقرة الأولى وارتكب بسبب ممارسة مهنة تهدف إلى توعية الجمهور، والعمل في مجال البحث العلمي⁽¹⁾.

ونص قانون تكنولوجيا المعلومات الهندي الصادر 2008⁽²⁾ في المادة (F66) على عقاب الإرهاب الإلكتروني إلى السجن مدى الحياة⁽³⁾.

(¹) **Art. 421-2-5-2** (L. no 2017-258 du 28 févr. 2017, art. 24) Le fait de consulter habituellement et sans motif légitime un service de communication au public en ligne mettant à disposition des messages, images ou représentations soit provoquant directement à la commission d'actes de terrorisme, soit faisant l'apologie de ces actes lorsque, à cette fin, ce service comporte des images ou représentations montrant la commission de tels actes consistant en des atteintes volontaires à la vie est puni de deux ans d'emprisonnement et de 30 000 € d'amende lorsque cette consultation s'accompagne d'une manifestation de l'adhésion à l'idéologie exprimée sur ce service.

Constitue notamment un motif légitime tel que défini au premier alinéa la consultation résultant de l'exercice normal d'une profession ayant pour objet d'informer le public, intervenant dans le cadre de recherches scientifiques ou réalisée afin de servir de preuve en justice ou le fait que cette consultation s'accompagne d'un signalement des contenus de ce service aux autorités publiques compétentes⁴.

(²) **The Information Technology ACT, 2008.**

(³) (F66) **Punishment for cyber terrorism:**

(1)Whoever,...

والقانون الإماراتي رقم 12 لسنة 2011 نص في المادة (٢٦) على عقوبة السجن والغرامة كل من أنشأ أو أدار موقعا إلكترونيا أو أشرف عليه أو نشر معلومات على الشبكة أو وسيلة تقنية، وذلك لجماعة إرهابية أو منظمة غير مشروعة بقصد تسهيل الاتصال بقياداتها أو أعضائها، أو لاستقطاب عضوية بها أو ترويج أفكارها.

كما نص القانون الكويتي رقم (63) لسنة 2015 في المادة (10) على أن يعاقب بالحبس مدة لا تجاوز عشر سنوات وبغرامة لا تقل عن عشرين ألف دينار ولا

(B) knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorized access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism.

(2) Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life".

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 قيادتها أو أعضائها, أو ترويج أفكارها, أو تمويلها, أو نشر كيفية تصنيع الأجهزة الحارقة, أو المتفجرة, أو أية أدوات تستخدم في الأعمال الإرهابية.

يجب على المشرع المصري النص بشكل صريح على تجريم استخدام تقنية المعلومات أو شبكة المعلوماتية أو موقع الإلكتروني أو موقع تواصل اجتماعي أي وسيلة نشر أو إعلان لتسهيل القيام بأعمال إرهابية أو لدعم جماعة أو منظمة تقوم بأعمال إرهابية أو لترويج أفكارها أو تمويلها, واعتبر ذلك من قبيل الأعمال الإرهابية المحظورة.

بما أنه يمكن استغلال مواقع التواصل الاجتماعي في ارتكاب جرائم من قبل جماعات منظمة, تدعو إلى نشر الفوضى والإخلال بالأمن الوطني, وترويج أفكار مضللة, والقيام بتجنيد عناصر تستهدف سيادة الدول واستقلالها ووحدة أراضيها.

لذلك لابد من وضع استراتيجية شاملة وفعالة في مواجهة الإرهاب عبر مواقع التواصل الاجتماعي, مع الأخذ في الاعتبار أوجه القصور والثغرات التي يستغلها الجماعات الإرهابية في إساءة استخدام الفضاء الرقمي سواء في ابتزاز الأفراد والشركات أو في نشر الأيديولوجيات المتطرفة, ولهذا يجب سد الفراغ التشريعي في القانون المصري لمكافحة هذه الظاهرة, وإنهاء حالة الإفلات من العقاب التي يتمتع

بها اليوم كثير من الناشطين الإرهابيين عبر مواقع التواصل الاجتماعي، وإيجاد أرضية مشتركة لصياغة منظومة قوانين دولية تتصدى لجذور الظاهرة الإرهابية عبر مواقع التواصل الاجتماعي.

ويجب النص على معاقبة أي شخص جنائياً إذا اشترك أو أنشأ أو استضاف مواقع أو بث صوراً تعرض على الإرهاب، سواء عن طريق الكتابة، أو المطبوعات، أو الرسومات، أو اللوحات، أو الشعارات، أو الصور، أو أي وسيلة أخرى من الكلام، أو الكتابة، أو الصور التي تباع أو توزع.

ضرورة وضع الآليات اللازمة لمراقبة المواقع وإنشائها وتنظيم ذلك، وخاصة مواقع التواصل الاجتماعي التي تُستخدم لنشر الأفكار السامة والهدامة التي تستخدم للأغراض الإرهابية وتعلم الإرهاب والوسائل المساعدة له وحجب المواقع التي تُشتبه بأنها تتبع جماعات إرهابية أو أنها ذات ميول إرهابية أو تخدم الجماعات الإرهابية بطريقة مباشرة أو غير مباشرة.

ضرورة العمل على تطوير وبناء قدرات أجهزة الأمن بالتعامل مع الجرائم الإلكترونية، خاصةً الإرهابية منها، والتدريب على مختلف الأنشطة وطرق مكافحة والوقاية منها، والكشف عنها والتعامل مع مسرح الجريمة والتحقيق فيها.

ويجب اتباع ضوابط وآداب التعامل مع مواقع التواصل الاجتماعي لمواجهة التطرف والإرهاب، فهذه التقنيات يمكن أن تستخدم في الخير كصلة الرحم وأعمال التسويق والتجارة.

الخاتمة

الحمد لله الذي بنعمته تتم الصالحات والصلاة والسلام على أشرف المرسلين سيدنا محمد صلى الله عليه وسلم ومن اهتدى بهداه إلى يوم الدين.

لقد تطورت الظاهرة الإجرامية في العصر الحديث تطوراً ملحوظاً، سواء في أشخاص مرتكبيها أو في أسلوب ارتكابها والذي يتمثل في استخدام آخر ما توصلت إليه العلوم التقنية والتكنولوجية وتطويعها في خدمة الجريمة، ولما كانت جرائم إساءة استخدام مواقع التواصل الاجتماعي ظاهرة إجرامية حديثة النشأة لتعلقها بتكنولوجيا الحاسب الألي فقد اكتنفها الغموض بالشكل الذي دعا إلى القول بأن جرائم إساءة استخدام مواقع التواصل أشبه بالخرافة.

حيث أتاحت الثورة التكنولوجية والعلمية وتطور استخدام شبكة الإنترنت أن أصبح استخدامها متاحاً للجميع، وإن كان يوصف العالم بأنه أصبح قرية صغيرة، إلا أن التطور المتسارع أصبح بموجبه العالم أصغر من القرية، وقد انتشرت مواقع للتواصل الاجتماعي على شبكة الإنترنت التي تضم مجموعة من المواقع الاجتماعية، مثل الفيس بوك الإنستجرام، وتويتر، وغيرها، وتعطي بدورها مجالاً لإنشاء حسابات شخصية عبر مواقعها، بالإضافة إلى التواصل مع الآخرين الذين تجمعهم نفس الاهتمامات والهوايات.

وتعتبر مواقع التواصل الاجتماعي اليوم هي بمثابة وسائل إعلامية من نوع خاص، عُرِفَت بالإعلام الجديد، ويجب أن تُعامل من حيث المسؤولية الجنائية معاملة وسائل الإعلام الأخرى، لاشتراكها في صفة العلانية والانتشار.

وأُتاحت هذه المواقع الاستخدام المجاني في الكثير من الجوانب الاجتماعية، وأهمها التواصل مع الأصدقاء وفي مقدمة تلك المواقع الفيسبوك الذي أصبح أكبر جمهورية على الكرة الأرضية بعد إن تجاوز عدد المشتركين المليارات، ومع الفوائد الجمه لاستخدام مواقع التواصل الاجتماعي في التعريف بالأنشطة ونشر الأخبار والمقالات والأبحاث والحوار الإيجابي مع الأصدقاء والأقارب، إلا أن ثمة من يسيء استخدام مواقع التواصل الاجتماعي في الدخول غير المشروع، والسب والقذف والتشهير، والنصب الاحتيال، والابتزاز، والإرهاب بهدف تحقيق مآرب شتى واصبح استخدام الفيسبوك سلاح ذو حدين فجانب الجوانب الإيجابية، أصبحت الأمور السلبية في مقدمة ما يخشى المشترك من استخدامه.

ولما كانت خاتمة البحث ليست مجرد ترديد لما يحويه البحث من تقسيمات، ولكنها انعكاسٌ لما توصلنا إليه، فقد أسفرت هذه الدراسة عن عدة توصيات سوف أوجزها على النحو التالي:

التوصيات:

فرضت مواقع التواصل الاجتماعي نفسها بشكل واضح وخصوصاً بين الشباب، فعلى الجميع توخي الحذر عند استخدام مواقع التواصل الاجتماعي وعدم إغفال مبادئ الشريعة الإسلامية والنظام العام، والتي من أبرزها تحري صحة ما ينشر وعدم نشر الفتن والردائل وما لا يفيد. ولابد من ترشيد استخدام مواقع التواصل الاجتماعي، والتحذير من مغبة إدمان استعمالها، حيث إن الشباب يضيع أوقاتاً كثيرة عبر هذه المواقع.

ضرورة مواكبة المستجدات بتعديل قانون مكافحة جرائم تقنية المعلومات في مصر، فلا شك أن التأثير المجتمعي الذي يحدثه التقدم التكنولوجي يحتاج إلى تعديل تنظيم قانوني، يضع إطاراً للعلاقات التي تترتب على استخدامه، بما يكفل حماية الحقوق، وتحديد الالتزامات، فلا بد من مواكبة القواعد القانونية للتقدم العلمي والتكنولوجي، فلا يجب على المشرع المصري أن يقف صامتاً مكتوف الأيدي حيال هذا التقدم، ولا يقف دور القانون على تنظيم العلاقات المترتبة على التقدم التكنولوجي، بل أنه يجب أن يحمي القيم والمبادئ عند استخدام مواقع التواصل الاجتماعي وتحديد المسار الصحيح الذي يجب أن يسلكه التقدم التكنولوجي، حتى لا يتخذ المجرمون أداة لتطوير وسائل إجرامهم، ومن هنا يجب على القانون أن تمتد نصوصه إلى الأنشطة الجديدة التي تفرزها التكنولوجيا.

ضرورة العمل على استثمار إيجابيات مواقع التواصل الاجتماعي، والتي من أبرزها الاستخدامات للأغراض التعليمية والاستخدامات الحكومية والتجارية، والحذر من سلبياتها كنشر أفكار هدامة وعمل تجمعات مخالفة للقيم والأخلاق.

نُهب المشرّع المصري بالنص صراحة على استخدام مواقع التواصل الاجتماعي في إجراءات التحري والتقصي عن الجرائم، فهو أسلوب ناجح في التحري عن الجرائم بمعرفة الشرطة من خلال تحليل المواقع لتحديد العلاقات بين المشتبه فيهم والجرائم الناشئة عن مواقع التواصل الاجتماعي.

نقترح بإنشاء حلقة اتصال محددة على شبكة الإنترنت تربط البنوك والمصرف المركزي في الدولة؛ حتى يمكن الاطلاع على حسابات العملاء مع عدم الإخلال بخصوصية حساباتهم، وعدم التماهي في فرض القيود على المصارف حتى لا تعوق العمليات المصرفية والتجارية، والتنسيق بين البنوك من خلال لقاءات وحوارات وندوات لمساعدة بعضها بعضاً على اتخاذ الإجراءات اللازمة لمواجهة جرائم تقنية، والجرائم المستحدثة فيها وصولاً إلى تحقيق أداء أفضل وتلافياً للأخطاء.

نوصي بضرورة إنشاء محاكم خاصة تتضمن في تشكيلها أحد المتخصصين في تقنية المعلومات للحكم في جرائم تقنية المعلومات.

عقد دورات تدريبية لأعضاء النيابة العامة وأفراد الشرطة خاصة، وأطلاعهم دائماً على المستجدات الحديثة في نطاق جرائم تقنية المعلومات، وتدريب جرائم تقنية المعلومات في كليات الحقوق والشريعة والقانون والشرطة.

ضرورة العمل على تطوير أجهزة الأمن للتعامل مع الجرائم الإلكترونية، خاصة جرائم الإرهاب، والتدريب على مختلف الأنشطة وطرق مكافحة والوقاية منها، والكشف عنها والتعامل مع مسرح الجريمة والتحقيق فيها.

ضرورة النص على مسئولية مزود خدمات الاستضافة عن المحتوى، إذا توافر لديه العلم الفعلي بطبيعته غير المشروعة، ولم يتصرف فوراً لإزالة البيانات، ولا سيما عند نشر معلومات أو بيانات على الموقع من شأنها تعريض أمن الدولة ومصالحها العليا للخطر أو المساس بالنظام العام، أو بقصد السخرية، أو الإضرار بسمعة أو هيبة أو مكانة الدولة أو أي من مؤسساتها أو رئيسها أو نائبه أو علم الدولة أو شعارها أو نشيدها الوطني، أو كانت تهدف أو تدعو إلى قلب نظام الحكم في الدولة أو تغييره أو الاستيلاء عليه، أو إلى تعطيل أحكام الدستور أو القوانين السارية في البلاد أو المناهضة للمبادئ الأساسية التي يقوم عليها نظام الحكم في جمهورية مصر العربية.

النص على إلزام مديري تحرير المواقع بإبلاغ مزودي خدمات الاستضافة بالعناوين والأسماء الخاصة بالبريد الإلكتروني للمستخدمين عند فتح الصفحة الشخصية لهم،

وهو الأمر الذي يقتضي تعهد المستخدم بصحة هذه البيانات وتحذيره بأن استخدام اسم غير حقيقي أو هوية مزورة من شأنه أن يعرضه للعقاب.

إنشاء قسم لتلقي بلاغات التحرش الافتراضي والتغريب بالأطفال عبر الإنترنت، حيث يمكن استغلال مواقع التواصل الاجتماعي في استدراج الأطفال، وابتزازهم، باستغلال ضعف الإدراك لديهم، وعدم قدرتهم على التمييز، ما يجعل ابتزازهم والتغريب بهم سهلاً؛ لأن أجهزة الاتصال بالإنترنت تقدم بيئة خصبة للجرائم الموجهة ضد الأطفال بسبب صعوبة وقوعها تحت رقابة الأسرة.

ضرورة النص على معاقبة كل من أنشأ على مواقع التواصل الاجتماعي صفحات تستغل في نشر أو إعادة نشر أو كتابة أو تدوين أو صياغة معلومات، أو بيانات، أو صور، أو أفلام، أو مستندات، أو أرقام، أو حروف، أو رموز، أو إشارات وغيرها، وجعلها متاحة لمستخدمي الإنترنت، أو سهل للغير ذلك، كل من قام بالصياغة أو الكتابة أو التدوين أو الإرسال لأي شيء بهدف ارتكاب جرائم إرهابية. وتشديد العقوبة إذا كان المنشور معلومات، أو بيانات، أو صوراً، أو أفلاماً، أو مستندات، أو أرقاماً، أو حروفاً، أو رموزاً، أو إشارات وغيرها، مما يتصل بأسرار الدولة العسكرية أو يضر بالأمن القومي لها أو يهدد مصالحها الاقتصادية.

نعتقد ضرورة تعديل القانون المصري رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات، على معاقبة كل من أنشأ على مواقع التواصل الاجتماعي صفحات تستغل في نشر أو إعادة نشر أو كتابة أو تدوين أو صياغة معلومات، أو

بيانات، أو صور، أو أفلام، أو مستندات، أو أرقام، أو حروف، أو رموز، أو إشارات وغيرها، أو جعلها متاحة لمستخدمي الإنترنت، أو سهل للغير ذلك. كما يعاقب بالعقوبة ذاتها كل من قام بصياغة أو كتابة أو تدوين أو إرسال شيء مما ذكر، وتكون العقوبة السجن المؤبد إذا كانت تلك المعلومات، أو البيانات، أو الصور، أو الأفلام، أو المستندات، أو الأرقام، أو الحروف، أو الرموز، أو الإشارات تتصل بأسرار الدولة العسكرية أو الأمنية أو تهدد مصالحها الاقتصادية.

عقاب كل من أنشأ أو أدار موقعاً إلكترونياً، أو أشرف عليه أو نشر معلومات في الشبكة المعلوماتية أو في أي وسيلة تقنية معلومات، وذلك لجماعة إرهابية أو أي مجموعة أو جمعية أو منظمة أو هيئة غير مشروعة بقصد تسهيل الاتصال بقياداتها، أو ترويج أو تحبيذ أفكارها، أو تمويل أنشطتها، أو توفير المساعدة الفعلية لها، أو بقصد نشر أساليب.

وكل من أنشأ أو أدار موقعاً إلكترونياً أو أشرف عليه أو استضاف موقعاً إلكترونياً، أو قدم خدمات تقنية تتعلق بالشبكة المعلوماتية، أو استخدم معلومات على الشبكة المعلوماتية أو في أي وسيلة تقنية معلومات بقصد التحريض على أفعال، أو نشر أو بث معلومات أو أخباراً أو رسوماً كرتونية أو أي صور أخرى، من شأنها تعريض أمن الدولة ومصالحها العليا للخطر أو المساس بالنظام العام.

نرى أنه يجب إدراج نص في القانون رقم 175 لسنة 2018 على أن "يعاقب بالحبس مدة لا تقل عن سنتين وغرامة لا تقل عن ثلاثمائة ألف جنيه ولا تجاوز

خمسمائة ألف جنيه، كل من يقوم بالإعلانات الوهمية عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات أو أحد مواقع التواصل الاجتماعي إلى الاستيلاء لنفسه أو لغيره على مال مملوك للغير أو على سند أو على أدوات إنشاء توقيع إلكتروني خاص بالغير، وكان ذلك للاستيلاء على عقار مملوك للغير أو بعضه".

نقترح على المشرع المصري إضافة نص في قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018 على أن "يعاقب بالسجن مدة لا تقل عن ثلاث سنوات وبغرامة لا تقل عن خمسين ألف ولا تزيد على مائة وخمسين ألف جنيه كل من استخدم موقع إلكتروني أو موقعاً للتواصل الاجتماعي أو وسيلة من وسائل تقنية المعلومات في تهديد أو ابتزاز شخص طبيعي أو اعتباري لحمله على القيام بفعل أو الامتناع عنه. وإذا كان التهديد بارتكاب جناية أو يعد مساساً بالكرامة الإنسانية أو خادشاً للشرف والاعتبار والسمعة كانت العقوبة السجن وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز مائتين ألف جنيه، وتُشدّد العقوبة في حالة وقوع الجريمة على طفل أو عديم الأهلية".

نقترح على المشرع المصري بتعديل القانون رقم 175 لسنة 2018 بأن ينص صراحة على تجريم انتحال الشخصية على شبكة الإنترنت، ومواقع التواصل الاجتماعي، أو إحدى وسائل تقنية المعلومات.

ضرورة النص على تجريم الإرهاب عبر مواقع التواصل الاجتماعي من خلال نصوص خاصة في قانون تقنية المعلومات الذي سيتم إصداره، وذلك لمواكبة التطور التقني المستمر لهذه الجريمة.

وضع استراتيجية وطنية للأمن الإلكتروني وبشكل خاص إنشاء مركز للاستجابة السريعة لطوارئ الحاسب الآلي والإنترنت، ومكافحة الجرائم الإلكترونية.

ضرورة تشجيع الأشخاص وتحفيزهم على الإبلاغ عن الجرائم الإلكترونية بشكل عام والإرهاب بشكل خاص لخطورته على أمن المجتمع واستقراره.

معاينة أصحاب المواقع القائمة على ترويج الأفكار الهدامة وتبث الإشاعات التي من شأنها خلق الفتنة، سواء كانت هذه المواقع لأفراد أو مؤسسات.

تفعيل التعاون الدولي لمحاصرة الجرائم الإرهابية على شبكة الإنترنت، عن طريق تبادل المعلومات، والتعاون القضائي، وتسليم المجرمين.

إنشاء مواقع إلكترونية وصفحات على مواقع التواصل الاجتماعي لمجابهة الجرائم.

ضرورة وضع ضوابط وآداب التعامل مع مواقع التواصل الاجتماعي لمواجهة التطرف والإرهاب، فهذه التقنيات يمكن أن تستخدم في الخير كصلة الرحم وأعمال التسويق والتجارة.

نقترح على المشرع المصري إضافة نص في قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018 على أن "يعاقب بالسجن مدة لا تقل عن ثلاث سنوات وبغرامة لا تقل عن خمسين ألف ولا تزيد على مائة وخمسين ألف جنيه كل من استخدم موقع إلكتروني أو موقعاً للتواصل الاجتماعي أو وسيلة من وسائل تقنية المعلومات في تهديد أو ابتزاز شخص طبيعي أو اعتباري لحمله على القيام بفعل أو الامتناع عنه. وإذا كان التهديد بارتكاب جريمة أو يعد مساساً بالكرامة الإنسانية أو خادشاً للشرف والاعتبار والسمعة كانت العقوبة السجن وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز مائتين ألف جنيه، وتُشدّد العقوبة في حالة وقوع الجريمة على طفل أو عديم الأهلية".

ضرورة أن تعمل الدولة على تيسير التعاون الدولي في إطار الاتفاقيات الدولية والإقليمية والثنائية التي تم التصديق عليها، أو تطبيق مبدأ المعاملة بالمثل، بهدف تبادل المعلومات بما يكفل منع ارتكاب جرائم تقنية المعلومات، والمساعدة على التحقيق فيها وتتبع مرتكبيها.

إدخال مادة "جرائم تقنية المعلومات" في مناهج التدريس لطلبة كلية الحقوق والشريعة والقانون والشرطة، كمادة مستقلة، وذلك حتى يستطيع الدارسون التعرف على هذه الجرائم والإلمام بها.

حث الجامعات والمراكز البحثية للبحث والدراسة في جرائم تقنية المعلومات، وإنشاء
دبلومات متخصصة في المجالات الفنية والقانونية المتعلقة بمكافحة جرائم تقنية
المعلومات.

قائمة المراجع

أولاً: المراجع باللغة العربية:

- د/حسين بن سعيد بن سيف الغافري، السياسة الجنائية في مواجهة جرائم الإنترنت، دراسة مقارنة، رسالة دكتوراه كلية حقوق جامعة عين شمس، دون سنة نشر.
- د/ زاهر راضي، استخدام مواقع التواصل الاجتماعي في العالم العربي، مجلة التربية، جامعة عمان الأهلية، 2003.
- عبد الرزاق محمد الدليمي، الإعلام الجديد والصحافة الإلكترونية، دار وائل للنشر، الطبعة الأولى، الأردن، 2011.
- د/ مجدي محمد عبد الجواد الداغر، استخدامات الإعلاميين لشبكات التواصل الاجتماعي والإشباع المتحققة، دراسة تطبيقية على القائم بالاتصال بالمؤسسات الإعلامية بالسعودية، مجلة كلية الآداب، جامعة الزقازيق، العدد 64، مارس 2013.
- د/ ياسر بكر، الإعلام البديل، مطابع حواس للنشر والتوزيع، القاهرة، 2010.

ثانياً: المراجع باللغة الفرنسية:

❖ **Français Références:**

▪ **Anne-Catherine Muller:**

– **Communications à destination des actionnaires individuels, Revue des sociétés, N° 01 du 08/01/2016.**

▪ **Bernard Bouloc:**

– **Collecte illicite de données nominatives, RTD Com, N° 04 du 15/12/2006.**

▪ **Bertrand de Lamy:**

– **La lutte contre le terrorisme à l'épreuve du contrôle de constitutionnalité: utiles précisions sur la nécessité d'une incrimination, RSC, N° 02 du 11/08/2017.**

▪ **Denis Baresch:**

– **Sécurité et confiance dans la communication électronique – pour une approche européenne, Revue du Marché commun et de l'Union européenne, N° 420 du 10/07/1998.**

- **Delphine Castel:**

– Réseaux sociaux – Comment Internet transforme la politique pénale, JA , N° 600 du 01/06/2019.

- **Emmanuelle Maupin:**

Recommandations sur l'utilisation des réseaux sociaux par les magistrats administratifs, AJDA, N° 15 du 22/04/2019.

- **Emilie Bailly & Emmanuel Daoud:**

–Cybercriminalité et réseaux sociaux: la réponse pénale, AJ Pénal, N° 05 du 14/05/2012

- **Étienne Dreyfous & Jean Wahl:**

–Questions–clés posées à l'Europe par les progrès des nouvelles technologies de l'information, Revue du Marché commun et de l'Union européenne, N° 416 du 10/03/1998.

- **Fabrice Mattatia:**

L'usurpation d'identité sur internet dans tous ses états, RSC, N° 02 du 14/08/2014.

- **François–Guillaume Lassemlée–Léon& Aurélia Marie:**

-La contrefaçon sur internet: nouvelles difficultés, nouveaux enjeux, AJ Pénal, N° 05 du 14/05/2012.

▪ **Frédéric Pollaud-Dulian:**

- Programmes d'ordinateur. Épuisement du droit de distribution. Revente d'occasion de copies. Supports physiques qui ne sont pas d'origine. Exceptions au droit de reproduction du logiciel, RTD, N° 04 du 19/01/2017.

-Exception de copie privée, RTD, N° 02 du 15/06/2007

- Protection juridique des mesures techniques de protection ou d'information. Echanges de «pair à pair». Téléchargement illicite. Sanctions pénales. Logiciels d'échanges. Autorité de régulation des mesures techniques, RTD, N° 02 du 15/06/2007

▪ **Géraldine Péronne& Emmanuel Daoud:**

-Discriminations et réseaux sociaux, AJ Pénal, N° 12 du 11/12/2014.

▪ **Jacques Francillon:**

– Application à la télématique et à l'Internet des règles de responsabilité propres au droit de la presse et de la communication audiovisuelle, RSC, N° 03 du 15/09/1999.

– De diverses variétés de piratages, RSC, N° 01 du 16/03/1998.

Messages racistes ou antisémites postés sur le réseau social Twitter, RSC, N° 03 du 20/11/2013.

– Piratage audiovisuel. Captation frauduleuse de programmes de télévision cryptée à péage, RSC, N° 01 du 16/06/2014.

– Piratage informatique. Collecte de renseignements commerciaux. Délit de maintien frauduleux dans un système de traitement automatisé de données, RSC, N° 01 du 14/03/2008, p.99.

– Piratage informatique. Usurpation d'identité numérique.
L'affaire du « faux site officiel » de Rachida Dati: une étape dans la lutte contre la cyberdélinquance, RSC, N° 01 du 21/05/2015.

▪ **Jacques Larrieu & Christian Le Stanc & Pascale Tréfigny:**

– Droit du numérique, Recueil Dalloz, N° 37 du 31/10/2013.

▪ **Jean Cazeneuve:**

– La cybercriminalité: l'émergence d'un nouveau risque, N° 05 du 14/05/2012.

▪ **Jean-Pierre Gridel:**

– Sophie Sontag-Koenig, Technologies de l'information et de la communication et défense pénale, RTD Civ, N° 04 du 19/12/2014.

▪ **Jérôme Bossan:**

– Le droit pénal confronté à la diversité des intermédiaires de l'internet, RSC, N° 02 du 16/08/2013.

- **Jérôme Huet:**

- Site internet, flux RSS, responsabilité du rediffuseur, Recueil Dalloz, N° 15 du 15/04/2010.

- **Laurence Usunier:**

- La compétence des juridictions françaises pour connaître du différend entre le réseau social Facebook et l'un de ses membres, RTD Civ, N° 02 du 20/06/2016.

- **Nicolas Verly:**

- Diffamations et injures publiques sur les réseaux sociaux: définitions, responsabilités et sanctions, AJ Collectivités Territoriales, N° 12 du 16/12/2014.

- **Pascal Penaud:**

- Nouvelles technologies de l'information: quel impact sur les organismes de Sécurité sociale, Droit social, N° 09–10 du 10/09/199.

- **Pierre–Henri Conac:**

– Communication des sociétés cotées sur leur site internet et sur les médias sociaux, Revue des sociétés, N° 01 du 09/01/2015.

▪ **Pierre–Yves Verkindt:**

–Nouvelles technologies de l'information et de la communication et nouvelles pratiques d'expertise, Droit social, N° 01 du 10/01/2002.

▪ **Présidence et mot d'accueil:**

– Rôle et responsabilité des plateformes en ligne: approche(s) transversale(s) ou approches sectorielles?, Master 2 «Droit du commerce électronique et de l'économie numérique», Ecole de droit de la Sorbonne, Université Panthéon–Sorbonne (Paris I) ,IRJS, Département Sorbonne immatériel,24 novembre 2016 14h–19h, Salle des conférences, Lycée Henri IV, 23 rue Clovis, 75005 PARIS.

▪ **Sébastien Defix:**

– Réseaux sociaux et règles de propagande électorale, AJ Collectivités Territoriales, N° 12 du 16/12/2014.

- **Sophie André & Camille Lallemand:**

- Facebook contre le consommateur français: l'hallali de la clause attributive, Dalloz IP/IT 2016.

- **Sophie Prétot:**

- L'ami des réseaux sociaux: précisions sur l'appréhension juridique de la communauté virtuelle, Dalloz actualité, 19 janvier 2017.

- **Yves Mayaud:**

- Un attendu de principe pour le délit d'usurpation d'identité, RSC, N° 01 du 12/05/2016.

Journal Officiel:

- **JORF** n°0051 du 1 mars 2017, texte n° 3, LOI n° 2017-258 du 28 février 2017 relative à la sécurité publique.

- **JORF** n°0088 du 14 avril 2016, texte n° 1, LOI n° 2016-444 du 13 avril 2016 visant à renforcer la lutte contre le système prostitutionnel et à accompagner les personnes prostituées.

- **JORF** n°0129 du 4 juin 2016, texte n° 1, LOI n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale.
- **JORF** n°0171 du 26 juillet 2015 page 12735, texte n° 2, LOI n° 2015-912 du 24 juillet 2015 relative au renseignement.
- **JORF** n°0263 du 14 novembre 2014 page 19162, texte n° 5, LOI n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme .
- **JORF** n°0075 du 28 mars 2012 page 5604, texte n° 2, LOI n° 2012-410 du 27 mars 2012 relative à la protection de l'identité.
- **JORF** n°0062 du 13 mars 2012 page 4533, texte n° 16, Ordonnance n° 2012-351 du 12 mars 2012 relative à la partie législative du code de la sécurité intérieure.

- **JORF** n°0197 du 26 août 2011 page 14473, texte n° 49, Ordonnance n° 2011-1012 du 24 août 2011 relative aux communications électroniques.
- – **JORF** n°0143 du 22 juin 2004 page 11168, texte n° 2, Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.
- – **JORF** n°0263 du 14 novembre 2014 page 19162, texte n° 5, LOI n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme .
- – **JORF** n°170 du 23 juillet 1996 page 11104, LOI no 96-647 du 22 juillet 1996 tendant à renforcer la répression du terrorisme et des atteintes aux personnes dépositaires de l'autorité publique ou chargées d'une mission de service public et comportant des dispositions relatives à la police judiciaire.

Jurisprudence:

- Cour de cassation, Chambre criminelle, 7 février 2017, N° 15-83439

- Cour de cassation, Chambre criminelle, 14-03-2006, n° 05-83.423.
- Cour de cassation, Chambre criminelle, 06-09-2016, n° 15-86.412.
- Cour de cassation, Chambre criminelle, 02-11-2016, n° 15-87.163.
- Cour d'appel de Paris, pôle 2, ch. 2, 12-02-2016, n° 15/08624
- Tribunal de grande instance de Nanterre, 1re ch, 25-06-2009, n° 08/05405.

ثالثاً: المراجع الإنجليزية:

- **Andrew T. Stephen & Jeff Galak:**
 - The Effects of Traditional and Social Earned Media on Sales: A Study of a Microlending Marketplace, Journal of Marketing Research, 49, 4 April 2012.
- **Frank T. Piller & Alexander Vossen:**
 - From Social Media to Social Product Development: The Impact of Social Media on Co-Creation of Innovation, Die Unternehmung, Vol. 65, No. 1, 2012.

- **Hailiang Chen&Prabuddha De:**
 - Wisdom of Crowds: The Value of Stock Opinions Transmitted Through Social Media, Review of Financial Studies (RFS), Forthcoming, 04 Oct 2016.

- **Gerald C. Kane& Maryam Alavi:**
 - What's Different About Social Media Networks? A Framework and Research Agenda, MIS Quarterly, Forthcoming, 25 Mar 2013.

- **José van Dijck& Thomas Poell:**
 - Understanding Social Media Logic, Media and Communication, Vol. 1, Issue 1, 13 Aug 2013.

- **Khim Yong Goh &Cheng–Suang Heng & Zhijie LIN:**
 - Social Media Brand Community and Consumer Behavior: Quantifying the Relative Impact of User– and Marketer–Generated Content, 31 October 2012.
 -

- **Nikita Barman:**

- Legal Implications of Cyber Crimes on Social Networking Websites, International Journal of Scientific and Research Publications, Volume 5, Issue 12, December 2015.

- **Sarah Oates and Wendy W. Moe:**

- Donald Trump and the 'Oxygen of Publicity': Branding, Social Media, and Mass Media in the 2016 Presidential Primary Elections, Paper prepared for the American Political Science Association Annual Meeting Political Communication Section, 31August, 2016.