المسئولية الجنائية الناشئة عن إساءة استخدام مواقع التواصل الاجتماعي

إعداد

د/ دينا عبد العزيز فهمي

بحث مقدم للمؤتمر العلمي الرابع لكلية الحقوق جامعة طنطا

تحت عنوان

القانون والإعلام

المقرر انعقاده 23-24 إبريل 2017 م

مقدمـــــة

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 المعلومات والإعلام، وأدت هذه الثورة إلى تراكم مذهل 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 شبكات 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.

وإذا كانت مواقع التواصل الاجتماعي توفر الجهد والوقت والمال في جمع المعلومات، فمن خلالها يمكن التوصل إلى جميع أنواع المعلومات الشخصية الخاصة بالفرد أيضاً، 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 التهديدات خلال السنوات الأخيرة واعتمادها على التقنيات الحديثة والفضاء الإلكتروني والمعلوماتي، أصبح من الضروري وضع الأطر والتشريعات القانونية التي تكفل حماية كل ما يهدد الدولة في هذا الشأن.

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 الذى يصبو إليه جموع المصريين، ولعل أبرز ما نواجه في هذه المرحلة من التقدم والتنمية هي جرائم تقنية المعلومات والجريمة الإلكترونية والمعلوماتية التي تهدف إلى تدمير كيان المجتمع وتعصف بأمنه واستقراره وتعوق مسيرة التقدم والازدهار، لذا كان لزامًا 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 والبناء في نطاق الدستور والقانون.

وفي 2014 انضمت جمهورية مصر العربية إلى الاتفاقية العربية لمكافحة جرائم تقنية المعلومات[1], ووضع المشرع الفرنسي العديد من النصوص لمكافحة جرائم تقنية المعلومات, والقانون الإماراتي لمكافحة جرائم تقنية المعلومات, للمرسوم بقانون اتحادي في دولة الإمارات العربية المتحدة رقم (5) لسنة 2012 في شأن تقنية المعلومات[2] ووضع قواعد تحد من مخاطر هذه الشبكات, والقانون الكويتي رقم (63) لسنة 2015 في شأن مكافحة جرائم تقنية المعلومات[3].

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, ويلاحَظ في الآونة الأخيرة أنه يتم استغلال هذه المواقع في إثارة الشعوب وإحداث فوضى سياسية.
- تعتبر مواقع وشبكات التواصل الاجتماعي اليوم بمثابة وسائل إعلامية, تعرف بالإعلام الجديد, تعد اليوم أهم السمات البارزة, التي يستطيع الشخص استخدامها وكتابة منشوراته ونشر مقاطعه الصوتية أو المرئية وهو في أي مكان في العالم, وقد نتج عن ذلك تجاوزات, ومن ثم يتعين التصدي لها.
- تحديد المسئولية 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 يباشر خدمات تقنية تتمثل في توصيل خدمة الاتصال ولا علاقة له بالبيانات، أو المعلومات، التي يتم نشرها على هذه المواقع، أم هو الناشر الإلكتروني باعتباره محرِّر الموقع ويقوم بصياغة المعلومات، ويتحكم في البيانات التي يتم نشرها على صفحات مواقع التواصل الاجتماعي؟ وقد يجتمع الأمران معاً بأن

---

(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) - مرسوم بقانون اتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات.

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

يصبح منشئ الموقع هو ذاته الذي أُنيط به تحرير المحتوى , فمن المسئول عن المعلومات الواردة في ذلك المحتوى إذا تضمنت الإساءة إلى مستخدمي تلك المواقع؟

منهج البحث:

نظراً لعدم وجود تنظيم قانوني لهذا الموضوع, اعتمد البحث على المنهج المُقارن بالمقارنة بين بعض التشريعات, هذا بالإضافة إلى الاستعانة بالمنهج التحليلي من تحليل النصوص القانونية التي لها صلة بالبحث, والمشكلات التي نتجت عنه.

خطة البحث:

المبحث الأول: ماهية مواقع التواصل الاجتماعي

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

المبحث الأول

ماهية مواقع التواصل الاجتماعي

تمثل وسائل التواصل الاجتماعي ثورة رقمية نتيجة استخدامها في نشر المعلومات، فالمستخدم يمكن له نشر برامج، أو مؤلفات على صفحات الويب، وإبرام صفقات تجارية، والتواصل مع أقرانه، والتنقل بين أرجاء العالم، الأمر الذي جعل هذه الشبكات 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 والمعلومات, بما أتاحته من حرية وسرعة متابعة الحدث على مدار الساعة, وبما قدمته من خدمات متعددة من مواقع ومنتديات

---

(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.

وتصفح, حيث أدى ذلك إلى زيادة دور شبكات التواصل الاجتماعي, باعتبارها وسائل حرة للتعبير والتفاعل والتواصل بين أفراد المجتمع.

المطلب الأول

تعريف وأنواع مواقع التواصل الاجتماعي

تقسيم: نتطرق في هذا المطلب إلى تعريف مواقع التواصل الاجتماعي, ثم بيان أنواعه على النحو التالي:

الفرع الأول: تعريف مواقع التواصل الاجتماعي.

الفرع الثاني: أنواع مواقع التواصل الاجتماعي.

الفرع الأول

تعريف مواقع التواصل الاجتماعي

وقد عرّف **المشرع الفرنسي** التواصل الاجتماعي عبر شبكة الإنترنت في المادة الرابعة من القانون رقم 575 – 2004الصادر 21 يونيو 2004[1] بأنه بروتوكول اتصال مفتوح، أو ربط بيانات وتبادلها بأي شكل يصل إلى الجمهور دون قيد على أي محتوى تبادلي من قبل مقدمي الخدمات التقنية[2].

عرف القانون الإماراتي رقم(5) لسنة 2012 **الموقع الإلكتروني** بأنه مكان إتاحة المعلومات الإلكترونية على الشبكة المعلوماتية, ومنها مواقع التواصل الاجتماعي, والصفحات الشخصية والمدونات[3].

كما عرف القانون الكويتي رقم (63) لسنة 2015 **الموقع** بأنه مكان إتاحة المعلومات على الشبكة المعلوماتية من خلال عنوان محدد. و**إلكتروني** 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.

---

[1]-**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.

[2] - "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".

[3] المادة الأولى من القانون الإماراتي.

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 الكويتي.

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 انتماء (بلد، جامعة، مدرسة، شركة... إلخ)، كل هذا 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 يدونوها وعرض الصور, والاتصال بالأصدقاء الذين تعرفوا عليهم عن طريق الإنترنت أو في الواقع الحقيقي ومشاهدة البيانات الشخصية للآخرين.

وسائل التواصل الاجتماعي هي عبارة عن مجموعة من مواقع الاتصال عبر الإنترنت، وهذه الموقع 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. وللاشتراك بهذه الواقع ليس عليك إلا التسجيل من خلال الإيميل بكل سهولة لتصبح أحد المشتركين بهذه الوسائل المختلفة، التي تفتح أمامك العالم.

خصائص مواقع التواصل الاجتماعي:

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

---

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

1- **العالمية:** تلغى الحواجز الجغرافية والمكانية، وتتحطم فيها الحدود الدولية، حيث يستطيع الفرد في الشرق التواصل مع الفرد في الغرب، في بساطة وسهولة.

2- **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، فهي تلغي السلبية المقيتة في الإعلام القديم – التلفاز والصحف الورقية وتعطي حيزًا للمشاركة الفاعلة من المشاهد والقارئ.

3- **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.

4- **المجانية:** اقتصادية في الجهد والوقت والمال، في ظل مجانية الاشتراك والتسجيل، فالفرد البسيط يستطيع امتلاك حيز على الشبكة للتواصل الاجتماعي، وليست ذلك حكرًا على أصحاب الأموال، أو حكرًا على جماعة دون أخرى.

5- **الحرية المطلقة:** فمواقع التواصل الاجتماعي جعلت بإمكانية 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.

6- **سهولة الاستخدام:** لا يحتاج التعامل مع مواقع التواصل الاجتماعي خبرة معلوماتية حتى يتم التفاعل مع محتواها, كما لا يحتاج رواد المواقع غلى 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].

الفرع الثاني

---

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

أنواع مواقع التواصل الاجتماعي

لقد 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, حيث يضم الإنترنت ملايين المواقع التي تتناول كافة المجالات السياسية والاقتصادية والاجتماعية, وغيرها, يجرى خلالها أشكال متنوعة من التواصل الاجتماعي, وأصبحت مواقع التعارف المعروفة بشبكات التواصل الاجتماعي[1] منها فيس بوك(facebook), تويتر(twitter),

---

(1) تعتبر مواقع التواصل الاجتماعي أحدى أنواع المواقع الخدمية, حيث تتعدد المواقع الإلكترونية إلى عدة أنواع وهي:
المواقع الإلكترونية التي تقوم بمهمات 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 تذيل المواضيع المنشورة فيها بعبارة "لمزيد من التفاصيل زورو 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 وتحدث 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 الأخرون, 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 وتنشر 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 لمتصفحيها على الإنترنت, فهي تقدم لهم برامج تساعدهم في القيام ببعض المهام, مثل تحرير الصور وتعديلها دون اللجوء تنصيب أو تحميل برامج أخرى, وتقوم بنفس الغرض على أجهزتهم 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 تؤدى مهام بسيطة ولكنها مطلوبة, وعادة ما تكون هذه المهام متعلقة بمواقع إلكترونية أو 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;

ماي سبيس(MySpace), وغيرها من مواقع التواصل الاجتماعي, والتطبيقات الداعمة للاتصال مثل الواتس آب(WhatsApp), فايبر(Viber), سكاي 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.

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

الفيس بوك (facebook)

يعد الفيس بوك من أشهر مواقع التواصل الاجتماعي على مستوى العالم, وقد تم إطلاقه في فبراير 2004 ومن مؤسسيه مارك زوكربيرج Mark ZUCKERBERG الذي كان طالباً في جامعة هارفارد من أبرز مؤسسي هذه المواقع، فقد كان له دور بارز في تسهيل تبادل المعلومات بين الطلاب في الجامعة عبر شبكة للتواصل الاجتماعي, وقد أحدثت مواقع تحولت لاحقاً للموقع الذي بات أشهر مواقع للتواصل الاجتماعي فيسبوك(Facebook).

فموقع الفيس بوك هو أحد مواقع التواصل الاجتماعي الحديث رغم أن عمره لا يزيد عن ثلاث عشرة سنوات, إلا أنه أصبح الأشهر والأكثر استخداماً وتأثيراً على مستوى العالم، ويمكن من خلال هذا الموقع أن يقوم المشترك بإضافة أصدقاء إلى ملفه الشخصي, بالإضافة إلى إمكانية الانضمام إلى مجموعات.

تويتر (twitter):

أشهر مواقع التواصل الاجتماعي، ويقدم خدمة التدوين المصغر والتي تسمح لمستخدميهِ بإرسال «تغريدات» من شأنها تلقي اعجاب المغردين الاخرين، بحد أقصى 140 حرف للرسالة

د/ مجدي محمد عبد الجواد الداغر, استخدامات الإعلاميين لشبكات التواصل الاجتماعي والإشباعات 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.

الواحدة. وذلك مباشرة عن طريق موقع تويتر أو عن طريق إرسال رسالة نصية قصيرة SMS أو برامج المحادثة الفورية أو التطبيقات التي يقدمها المطورون مثل الفيس بوك وTwitBird وTwitterrific وTwhirl وtwitterfox.

كانت بداية تويتر في أوائل عام 2006 كمشروع تطوير بحثي أجرته شركة Odeo الأميركية في مدينة سان فرانسيسكو، وبعد ذلك أطلقته الشركة رسمياً للمستخدمين بشكل عام في أكتوبر 2006. وبعد ذلك بدأ الموقع في الانتشار كخدمة جديدة على الساحة في عام 2007 من حيث تقديم التدوينات المصغرة، وفي أبريل 2007 قامت شركة Odeo بفصل الخدمة عن الشركة وتكوين شركة جديدة باسم Twitter. بدءاً من ديسمبر 2009 فإن جوجل سوف يقوم بعرض نتائج بحث فورية في محرك بحث جوجل لمدخلات المستخدمين الجديدة في تويتر[1].

يوتيوب (YouTube):

موقع ويب يسمح لمستخدميه برفع التسجيلات المرئية مجانا ومشاهدتها عبر البث الحي (بدل التنزيل) ومشاركتها والتعليق عليها وغير ذلك, أسسه في 14 فبراير سنة 2005م ثلاث موظفين سابقين من شركة باي بال هم تشاد هيرلي وستيف تشين وجاود كريم، في مدينة سان برونو، سان ماتيو، كاليفورنيا، ويستخدم تقنية برنامج أدوبي فلاش لعرض المقاطع المتحركة. ومحتوى الموقع يتنوع بين مقاطع الأفلام، والتلفاز، والموسيقى، والفيديو المنتج من قبل الهواة، وغيرها[2].

إنستجرام (Instagram):

هو تطبيق مجاني لتبادل الصور وشبكة اجتماعية أيضاً، أطلق في أكتوبر عام 2010, يتيح للمستخدمين التقاط صورة، وإضافة فلتر رقمي إليها، ومن ثم مشاركتها في مجموعة متنوعة من خدمات الشبكات الاجتماعية، وشبكة إنستغرام نفسها. وتضاف الصور على شكل مربع، على غرار Instamatic كوداك وصور بولاويد، على النقيض من نسبة أبعاد 4:3 تستخدم عادة بواسطة كاميرات الهاتف المحمول. ففي البداية كان دعم إنستجرام على الآي فون، والآي باد، والآي بود تاتش، في أبريل 2012 إضافة إنستجرام دعم الأندرويد (Android). يتم توزيعه عبر متجر آيتونز وجوجل بلاي[3].

المطلب الثاني

---

(1) https://ar.wikipedia.org
(2) https://ar.wikipedia.org
(3) https://ar.wikipedia.org

أهمية مواقع التواصل الاجتماعي

إن 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

من خلال تعريف مواقع التواصل وأنواعها يمكن بسهولة 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 بطبعه وبفطرته يتواصل مع الآخرين ولا يمكن له 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 هذه تفرض عليه العيش مع الآخرين لإشباع هذه الحاجات. أما الاحتياجات الاجتماعية فلا يمكن أن تقوم أساسًا دون تواصل إنساني مع المحيط الاجتماعي ولذلك فالإنسان كائن اجتماعي بطبيعته لا يمكن أن يعيش بمفرده.

أصبحت مواقع التواصل الاجتماعي مصدر من مصادر الأخبار لكثير من روادها، وهي أخبار تتميز بأنها من مصدرها الأول وبصياغة فردية حرة غالبًا، 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.

كما واكب ذلك تقدم هائل في الإمكانات 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].

الفرع الثاني

دور مواقع التواصل الاجتماعي في جمع الاستدلالات

جمع الاستدلالات في جرائم تقنية المعلومات, نتيجة لما تتميز به مواقع التواصل الاجتماعي من سهولة الحصول على المعلومات، كونها تُعد حقلاً خصباً للسلطات في الحصول على المعلومات، فمن هنا يثار تساؤل مهم عن مدى إمكانية استخدام هذه الشبكات في جمع الاستدلالات عن جرائم المعلومات.

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

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 البيانات.

يمكن استخدام مواقع التواصل الاجتماعي في التحقيقات، وفي فرنسا تُستخدم أحد مواقع التواصل الاجتماعي الفيس بوك[3] لجمع المعلومات والاستدلالات في القضايا[4], كجرائم

---

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

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

(3) **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.

(4) **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'expertiseNote de bas de page, Droit social, N° 01 du 10/01/2002, p.54.

الخطف، والتحريض على الانتحار أو الكراهية العنصرية، والتشهير، والاتجار في الأعضاء البشرية, والمواد المخدرة، وجرائم الاعتداء الجنسي على الأطفال.

ولذلك يمكن استخدام هذه المواقع والصفحات الشخصية في إجراءات جمع الاستدلالات عن الجرائم بمعرفة الشرطة، فمن خلال تحليل شبكات الفيس بوك يمكن تحديد العلاقات بين المشتبه فيهم والجرائم الناشئة عن مواقع التواصل الاجتماعي.

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 تتوافر الشروط التالية:

1-أن تقع جريمة من جرائم تقنية المعلومات.

2- توافر الأدلة الكافية على وقوع تلك 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 على الحق في الخصوصية, وضع الدستور المصري 2014 حدوداً تحفظ الحق في الخصوصية, حيث نصت المادة(57) على أن "للحياة الخاصة حرمة, وهي مصونة لا تمس وللمراسلات 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.

يجوز الاعتداد بالدليل المستمد من المعلومات التي تم الحصول عليها من شبكات التواصل الاجتماعي. 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.

المبحث الثاني

نطاق المسئولية الجنائية لإساءة استخدام مواقع التواصل الاجتماعي

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.

إلا أن هناك 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 وكذلك التنافس الرياضي وما يحدث بين الإعلاميين من إساءات.

وإذا كان البحث يقتصر على المسئولية الجنائية عن سوء استخدام مواقع التواصل الاجتماعي، في هذا الصدد أن نلقي الضوء على أهم الجرائم التي تنجمُ عن سوء استخدام هذه المواقع:

أولاً: النصب عبر مواقع التواصل الاجتماعي:

يقع النصب والاحتيال 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 الاحتيال الإلكتروني عبر الإنترنت لا يمكن حصرها[2].

الاحتيال الإلكتروني:

قد عرف القانون الكويتي رقم (63) لسنة 2015 في شأن مكافحة جرائم تقنية المعلومات **الاحتيال الإلكتروني** بأنه التأثير في نظام إلكتروني مؤتمت أو نظام معلوماتي

---

(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.

(2)- **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.

إلكتروني أو شبكة معلوماتية أو مستند أو سجل إلكتروني أو وثيقة تقنية معلوماتية أو نظام أو جهاز حاسب آلي أو توقيع إلكتروني أو معلومات إلكترونية ذلك عن طريق البرمجة أو الحصول أو الإفصاح أو النقل أو النشر لرقم أو كلمة أو رمز سري أو بيانات سرية أو خاصة أخرى, بقصد الحصول على منفعة دون وجه حق أو الإضرار بالغير[1], ولم يعرف القانون الإماراتي الاحتيال الإلكتروني.

وفي هذا الصدد المشرّع 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].

وعرفت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات **جريمة الاحتيال** بأنه التسبب بإلحاق الضرر بالمستفيدين والمستخدمين عن قصد وبدون وجه حق بنية الاحتيال لتحقيق المصالح والمنافع بطريقة غير مشروعة, للفاعل أو للغير, عن طريق: 1- إدخال أو تعديل أو محو أو حجب للمعلومات والبيانات؛ 2- التدخل في وظيفة أنظمة التشغيل وأنظمة الاتصالات أو محاولة تعطيلها أو تغييرها؛ 3- تعطيل الأجهزة والبرامج والمواقع الإلكترونية.

للقاضي سلطة تقديرية عند تحديد الطرق الاحتيالية 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[3]، 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[4].

---

(1) الفقرة الأخيرة من المادة الأولى من القانون الكويتي رقم (63) لسنة 2015 في شأن مكافحة جرائم تقنية المعلومات, صدر بقصر السيف في 20 رمضان 1436 هـ - الموافق 7 يوليو 2015.

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

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

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

انتحال الشخصية:

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

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 المتوافرة في النظام ونسخها واستغلالها.

وتجدر الإشارة إلى أن المشرِّع المصري لم يضع نصا صريحا يجُرِّم انتحال الشخصية عبر مواقع التواصل الاجتماعي، على خلاف المشرعون الإماراتي, والكويتي, والسعودي[1], فقد 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 الاتي لا تقل عن مائتين وخمسين ألف درهم ولا تجاوز 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 تجاوز ثلاث سنوات وبغرامة لا تقل عن ثلاثة آلاف دينا ولا تجاوز 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 متي 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

---

[1] المادة الرابعة من نظام مكافحة جرائم المعلوماتية. صدر نظام مكافحة جرائم المعلوماتية بقرار مجلس الوزراء رقم 79 وتاريخ 1428/3/7هـ، وتمت المصادقة عليه بموجب المرسوم الملكي الكريم رقم م/17 وتاريخ 1428/3/8هـ .

الشخص أو عنوانه لفتح حساب مصرفي جديد، أو إنشاء الشيكات المزورة باستخدام الاسم، ورقم الحساب البنكي، والحصول على شيكات[1].

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

لذلك يجب على المشرّع المصري أن يتدخل بالنص صراحة على تجريم انتحال الشخصية على شبكة المعلومات، ومواقع التواصل الاجتماعي, أو إحدى وسائل تقنية المعلومات.

الإعلانات الوهمية:

تعتبر الإعلانات الوهمية سبب من أسباب ازدياد جرائم انتحال الشخصية ثم استغلالها في ارتكاب جرائم احتيال، أو تشهير وقذف، كالإعلانات عبر البريد الإلكتروني غير المرغوب فيه (البريد المزعج) 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 وضع القانون النص على تجريم الإعلانات الوهمية، وكل تحايل على العنوان الإلكتروني للإنترنت باستخدام عنوان وهمي أو عنوان عائد إلى آخرين أو بأي وسيلة أخرى.

نرى بانه يجب على مواقع التواصل الاجتماعي تبنّي سياسة رفع دعاوى تعويض ضد المتهمين بالتعرض لمستخدمي مواقع التواصل الاجتماعي بالرسائل الوهمية غير المرغوب فيها.

ثانياً: السب والقذف عبر مواقع التواصل الاجتماعي:

---

[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.

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.

لم ينص المشرع المصري على تجريم السب والقذف عبر مواقع التواصل الاجتماعي[1], إلا أن التشريعات الأخرى[2] تدخلت بتجريم ذلك, وفي هذا الصدد 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 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".

كما 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

---

(1) قد جرمت القواعد العامة السب والقذف, 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 القذف أو السب الذي ارتكب بإحدى الطرق المبينة في المادة (171) طعناً 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 قذف 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 القذف أو السب الذي ارتكب بالطريق المبين بالفقرتين السابقتين طعناً في عرض الأفراد أو خدشاً لسمعة العائلات يعاقب بالعقوبة المنصوص عليها في المادة 308."

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".

(2) 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 أياً من الجرائم المعلوماتية الآتية:

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

تسجيل أو صورة أو مشهد, بقصد التشهير أو الإساءة إلى شخص آخر, أو الاعتداء على خصوصيته أو انتهاكها"

وقد ذهب اتجاه في الفقه الفرنسي[1] إلى اعتبار استخدام مواقع التواصل الاجتماعي في السب بمثابة انتهاك لحرية الرأي والتعبير, وكذلك أحكام القضائية[2].

ثالثاً: الدخول غير المشرع عبر مواقع التواصل الاجتماعي:

قد 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.

وقد عرف القانون الكويتي رقم(63) لسنة 2015 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[3].

لم ينص المشرع المصري على تجريم الدخول غير المشروع لمواقع التواصل الاجتماعي, فقد 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 جزءً منها بالسجن سنتين (القانون رقم 2015-912 الصادر 24 يوليو 2015، المادة 4)[4] وغرامة قدرها 60ألف يورو. وإذا ترتب على ذلك 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) [5] 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[1].

---

(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.

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

(3) المادة الأولى من القانون.

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

(5) - 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.

يتبين من المادة سالفة الذكر بانه 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, تزود 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 2014-1353 الصادر 13 نوفمبر 2014، المادة 16) لاستخراج أو حيازة أو نسخ أو نقل، بحذف أو تعديل عن طريق الاحتيال على البيانات التي تحتوي عليها (القانون رقم 2004-575 الصادر 21 يونيو 2004، المادة 45) عليها بالسجن خمس سنوات وغرامة150 ألف يورو €. وتشدد العقوبة لتصبح السجن لمدة سبع سنوات وغرامة قدرها 300 ألف يورو, وذلك في حالة ارتكاب الجريمة ضد نظام المعالجة الآلية للبيانات الشخصية المحفوظة على أجهزة الدولة[2].

وتُشدد العقوبة في حالة ارتكاب الجريمة من قبل جماعة إجرامية مُنظمة, وذلك ما أقرته المادة(323 – 1–4) من قانون العقوبات بأن (القانون رقم 2014-1353 الصادر 13 نوفمبر 2014)[3] يُعاقب العقوبة بالسجن لمدة عشر سنوات وغرامة300000 € يورو (القانون رقم 2015-912 الصادر24يوليو 2015، المادة 4) إذا ارتكبت الجرائم المنصوص عليها في

---

(1)- **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. nº 2004-575 du 21 juin 2004, art. 45-I) «deux ans» d'emprisonnement et de (L. nº 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. no 2015-912 du 24 juill. 2015, art. 4) «100 000 €» d'amende.

(L. no 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. nº 2015-912 du 24 juill. 2015, art. 4) «150 000 €» d'amende.»"

(2) **Art. 323-3** "Le fait d'introduire frauduleusement des données dans un système de traitement automatisé (L. nº 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. nº 2004-575 du 21 juin 2004, art. 45-III) «cinq ans» d'emprisonnement et de (L. nº 2015-912 du 24 juill. 2015, art. 4) «150 000 €» d'amende.

(L. nº 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. nº 2015-912 du 24 juill. 2015, art. 4) «300 000 €» d'amende.»"

(3) - 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 .

المواد 323-1 إلى 323-3-1 من قبل عصابات منظمة بدخول نظام المعالجة الآلية للبيانات الشخصية التي تم تخزينها على أجهزة الدولة"[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 تجاوز 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 أيّ بيانات أو معلومات. 3- تكون العقوبة الحبس مدة لا تقل عن 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[2]. كما جرمت الاتفاقية العربية لمكافحة تقنية المعلومات الدخول والبقاء والاتصال غير المشروع لكل أو جزء من تقنية المعلومات أو الاستمرار به[3].

---

(1) - **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. no 2015-912 du 24 juill. 2015, art. 4) «300 000 €» d'amende".

(2) 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 أرتكب أياً من الجرائم المنصوص عليها أعلاه أو سهل ذلك للغير وكان ذلك أثناء أو بسبب تأدية وظيفته".

(3) **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

يتبين لنا أن القانون الفرنسي والإماراتي والكويتي والاتفاقية العربية لمكافحة جرائم تقنية المعلومات نصوا على تجريم صور الدخول إلى موقع إلكتروني، أو نظام معلومات إلكتروني، أو شبكة معلومات، أو وسيلة تقنية معلومات، وتشدد 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 على تجريم الدخول غير المشروع لمواقع التواصل الاجتماعي.

عقوبة الشروع:

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 323-1 حتى 323-3-1 بذات العقوبات المنصوص عليها للجريمة[1].

العقوبات التكميلية:

ويخضع الأشخاص المدانين بالجرائم المنصوص عليها إلى العقوبات التكميلية التالية:

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

2- المنع من تولي مناصب عامة أو القيام النشاط الاجتماعي أو مهني الذي بممارسته أو بمناسبته ارتكبت الجريمة لمدة أقصاها خمس سنوات 131-27.

3- مصادرة الأشياء الذي استخدمت أو أعدت لارتكاب الجريمة أو الناتج عن الجريمة، باستثناء المواد الخاضعة للاسترداد, المادة131-21 من قانون العقوبات.

4- إغلاق المنشأة أو المؤسسة التي استخدمت لارتكاب الجريمة لمدة خمس سنوات، مؤسسات أو واحد 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.

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."

[1]- **Art. 323-7** " La tentative des délits prévus par (L. nº 2004-575 du 21 juin 2004, art. 46-II) «les articles 323-1 à 323-3-1» est punie des mêmes peines".

6- حظر إصدار أو سحب شيكات لمدة تصل إلى خمس سنوات، المادة 131-19 من قانون العقوبات.

7- إشهار أو نشر القرار الذي اتخذ وفقا للمادة 131-35 من قانون العقوبات[1].

العدوى عن طريق إرسال الفيروسات عبر مواقع التواصل الاجتماعي:

قد يكون الدخول مشروعاً, إلا أن الهدف منه يكون بغاية الإضرار بأجهزة الغير عن طريق إرسال فيروسات[2], يعتبر من أخطر الاعتداءات على الوسائل التقنية، العدوى عن طريق الفيروسات والبرمجيات الخبيثة التي تتسبب في إتلاف جهاز الكمبيوتر، أو تدمير البرامج، أو إتلاف البيانات[3].

فقد جرمت كافة التشريعات المنظمة لجرائم تقنية المعلومات الدخول غير المشرع, 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 آلياً، أو ضعف أداء هذا النظام.

---

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

1º 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;

2º 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.*

3º 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.*

4º La fermeture, pour une durée de cinq ans au plus, des établissements ou de l'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés; — Pén. 131-33.

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

6º 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.

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

(2) 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.

(3) - **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.

لذلك نرى ضرورة التوسع في نطاق التجريم ليشمل إرسال أي بيانات إلكترونية تحوي 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.

رابعاً: جرائم النشر الإلكتروني عبر مواقع التواصل الاجتماعي:

يتوقف النظام القانوني للمسئولية الجنائية في الجرائم الناشئة عن سوء استخدام مواقع التواصل الاجتماعي على التكييف القانوني للقائم بالتشغيل، وهي تقنية تسمى "تكنولوجيا وسيطة للإنترنت" وتتنوع المسئولية الجنائية بين مزود خدمات الاستضافة.

المقصود بالناشر الإلكتروني:

لا يوجد تعريف في نصوص القانون المقارن لناشر المحتوى في جرائم النشر الإلكتروني بخلاف "مقدمي خدمات استضافة المواقع"، نصت المادة (6) من القانون الفرنسي بشأن الاقتصاد الرقمي (LCEN) المُعدل بمقتضى القانون 2016-444 الصادر 13 إبريل2016[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 المستفيدين من تلك الخدمات.

وبالتالي يترك سلطة تقديرية واسعة في تحديد المراد بالناشر الإلكتروني, وقد عرف التقرير الصادر عن الجمعية الوطنية الفرنسية الناشرين بأنهم الأشخاص الذين يقومون بصياغة المعلومات أو تحريرها أو نشرها أو إعادة نشرها أو وضعها على مواقع التواصل الاجتماعي[2].

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

---

[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 .

[2]- Rapport d'information de l'Assemblée Nationale sur la mise en application de la loi no.2004-575 du 21 juin2004 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

بهم توصيل خدمات الاتصال مباشرة بالإنترنت[1]، وتخزين المعلومات؛ فهؤلاء مزودو خدمات استضافة، وليسوا ناشرين[2].

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

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 أنشا 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

---

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

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

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 تنطوي 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 عهودهم أو نواب حكام الإمارات أو علم الدولة أو السلام الوطني أو شعارها أو نشيدها الوطني أو رموزها[3].

ووضع المشرع الإماراتي نصوص تُجرِّم 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 الشبكة المعلوماتية[4]. أو وقع

---

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

النشر بقصد الاتجار في البشر أو الأعضاء البشرية، أو التعامل فيها بصورة غير مشروعة[1], 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[2], 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[3].

ويتضح من ذلك أن جرائم النشر الإلكتروني لم يشترط المشرع الاتحادي فيها صفة خاصة 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 مجنياً عليه عندما يقع التعدي على حقوق النشر المحفوظة له.

وكذلك من يتلقى تلك الرسائل على صفحته الشخصية أو على الموقع باعتبار أنه مصرَّح 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 تنطوي على جريمة أصبح مدير تحرير الموقع مسئولاً عنها، لأنه سمح بنشرها على موقعه، ومن ثم تنعقد المسؤولية الجنائية في حقه عما تضمنه هذا المحتوى. في حين أنه استناداً إلى المادة السالفة الذكر لن يعاقب؛ 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 ناشرا لأنه لم يدخل إلى الموقع بطريق غير مشروع، بينما

---

(1) المادة 23 من المرسوم بقانون اتحادي في شأن جرائم تقنية المعلومات.
(2) المادة 25 من المرسوم بقانون اتحادي في شأن جرائم تقنية المعلومات.
(3) المادة 26 من المرسوم بقانون اتحادي في شأن جرائم تقنية المعلومات.

المستقر عليه أنه يعد ناشراً إلكترونياً أيضاً من قام بإنشاء أو كتابة، أو تدوين، أو صياغة المحتوى من الأصل. أو من توافر لديه عنصرا 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 نص المشرع المصري في القانون الجديد في شأن 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.

تحديد المسئولية الجنائية في جرائم النشر الإلكتروني:

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

- يجب على مدير تحرير الموقع رصد ما يتم نشره على الموقع ومراقبته، باعتباره هو الذي قام بإنشاء صفحة التواصل على الموقع، ومن ثم تتوافر المسئولية في حقه عن نشر عبارات أو معلومات أو بيانات تشكل جريمة يعاقب عليها قانوناً إذ يُفترض في حقه العلم بما يتم نشره، إلى جانب مسئولية 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 المسئولية عن جرائم النشر بوصفها جريمة غير عمدية إذا ثبت أن مدير تحرير الموقع أهمل في واجب المراقبة والرصد لما يتم نشره، باعتبار أن من واجبه بذل العناية اللازمة في مراقبة هذه المعلومات ورصدها.

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 شبكات التواصل الاجتماعي بأن يُدرج اسم موقعه، ويحدد هويته على شبكة الإنترنت لإمكانية التعرف إليه 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 والقُصَّر.

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 الناشرون, وعند الخروج عن هذه الالتزامات تتوافر المسئولية الجنائية في حقهم[1]، وقد اعتمد المجلس الدستوري الفرنسي ذلك القانون من قبل الجمعية الوطنية ومجلس الشيوخ في 30 يونيو 2006، ونص على غرامات تبدأ من 300,000 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 ب 30000 يورو لأي شخص يوزّع أو يسهّل توزيع البرمجيات بمخالفة تدابير الحماية التقنية (DRM) لإدارة الحقوق الرقمية[2].

عقوبة جريمة النشر الإلكتروني:

عاقَب المشرعون الفرنسي الإماراتي والكويتي من يقوم بالدخول غير المشروع إلى نظام معلومات إلكتروني أو شبكة معلومات، أو وسيلة تقنية معلومات، من 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. وإذا وقعت الجريمة من الجاني بمناسبة أو بسبب تأدية عمله فتكون العقوبة الحبس مدة لا تقل عن سنة

---

(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.

واحدة، والغرامة التي لا تقل عن مائتين وخمسين ألف درهم ولا تتجاوز مليون درهم، أو بإحدى هاتين العقوبتين[1].

وإذا انتفى لدى الجاني القصد الجنائي فلا يعاقَب 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.

خامساً: المسئولية الجنائية لمقدمي الخدمات الإلكترونية عبر مواقع التواصل الاجتماعي:

عرفت 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[2].

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

وتنعقد المسئولية الجنائية عن جرائم النشر على مديري التحرير أو الناشرين، فهؤلاء هم المسئولون 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[3]. ولا تنعقد مسؤولية مزودي خدمات الاستضافة إلا في حالتين:

1 – إذا توافر لديهم العلم الفعلي بالطبيعة غير المشروعة للمحتوى، ولم يخطروا السلطات أو يتصرفوا فوراً لإزالة البيانات، أو جعل الوصول إليها مستحيلاً , المادة 2/ 6 من القانون الفرنسي بشأن الاقتصاد الرقمي[4].

---

[1] المادة(2) من المرسوم بقانون اتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات.

[2] 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.

[3] - **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.

[4] - **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,

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

التزامات مزودي خدمة الاستضافة:

1- يجب 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، يتعين على مزودي خدمات الاستضافة إبلاغ السلطات بعناوين هؤلاء الأشخاص، والبريد الإلكتروني والصفحة الشخصية، الأمر الذي يتعين معه إلزام مزودي خدمات الاستضافة مدير تحرير الموقع بالحصول على المعلومات الشخصية للمستخدمين مسبقاً عند إنشاء صفحات التواصل[1].

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

3- يجب على مقدمي الخدمات التقنية مراقبة المعلومات التي تشكل جريمة تهدّد 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, عدم 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.

ويسأل مزود الخدمة جنائياً ومدنياً عن أعمال التعدي على حقوق النشر والتأليف وإنتاج الفيديو؛ لأن المحتوى المتاح عبر الشبكة غير قانوني وتم سحبه من الشبكة من قبل المنتجين، ولهذا تنعقد المسئولية الجنائية في حقهم عن سحب المحتوى, ذلك وفقاً لقرار المجلس الدستوري الفرنسي[2].

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

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

[2] "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

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

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.

كما نرى ضرورة النص على معاقبة أي شخص جنائياً إذا اشترك أو أنشأ أو استضاف مواقع أو بث صوراً تحرض 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.

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 مسبقة 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.

الخاتمـــــة

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

أتاحت الثورة التكنولوجية والعلمية وتطور استعمال شبكة الإنترنت أن اصبح استخدامها متاحا للجميع وان كان يوصف العالم بانه اصبح قرية صغيرة إلا أن التطور المتسارع اصبح بموجبه العالم اصغر من القرية وفي شبكة الإنترنت انتشرت مواقع للتواصل الاجتماعي.

وتعتبر مواقع التواصل الاجتماعي الحديثة اليوم هي بمثابة وسائل إعلامية من نوع خاص، عُرفت بالإعلام الجديد, وتُعامل من حيث المسئولية الجنائية معاملة وسائل الإعلام الأخرى، لاشتراكها في صفة العلانية والانتشار.

وأتاحت هذه المواقع الاستخدام المجاني في الكثير من الجوانب الاجتماعية وأهمها التواصل مع الأصدقاء وفي مقدمة تلك المواقع الفيسبوك الذي اصبح أكبر جمهورية على الكرة الأرضية بعد إن تجاوز عدد المشتركين المليارات, ومع الفوائد الجمه لاستخدام مواقع التواصل الاجتماعي في التعريف بالنشاطات ونشر الأخبار والمقالات والأبحاث والحوار الإيجابي مع الأصدقاء والأقارب, إلا أن ثمة من يسيء استخدام مواقع التواصل الاجتماعي في الاحتيال والإساءة والتشهير والسب والقذف والسرقة بهدف تحقيق مارب شتى واصبح استخدام الفيسبوك سلاح ذو حدين فبجانب الجوانب الإيجابية, أصبحت الأمور السلبية في مقدمة ما يخشى المشترك من استخدامه.

ولِما 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 :

- ضرورة مواكبة المستجدات في الإعلام الجديد، من خلال الإسراع في إصدار قانون لمكافحة جرائم تقنية المعلومات في مصر.
- ضرورة إصدار تشريع يجرم ويكافح الجريمة الإلكترونية والقضاء على كل العناصر والكيانات من الوصول إلى أهدافها وإجهاض تحركاتها، ويختص القانون المقترح بمكافحة جرائم تقنية المعلومات وتنظيم حماية الفضاء الإلكتروني ومكافحة الجريمة الإلكترونية وأمن الفضاء المعلوماتي والجرائم المعلوماتية.
- نُهيب المشرِّع المصري على النص صراحة على استخدام وسائل التواصل الاجتماعي في إجراءات التحري والتقصي عن الجرائم، فهو أسلوب ناجح في التحري عن الجرائم بمعرفة

الشرطة من خلال تحليل الشبكات لتحديد العلاقات بين المشتبه فيهم والجرائم الناشئة عن وسائل 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 التمادي 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، واطْلاعهم دائماً على المستجدات الحديثة في نطاق جرائم تقنية المعلومات. وتدريس جرائم تقنية المعلومات في كليات الحقوق والشرطة.
- ضرورة النص على مسئولية مزود خدمات الاستضافة عن المحتوى، إذا توافر لديه العلم الفعلي بطبيعته غير المشروعة، ولم يتصرف فوراً لإزالة البيانات، ولاسيما 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 والتغرير بالأطفال عبر الإنترنت، إذ يمكن استغلال مواقع التواصل الاجتماعي في استدراج الأطفال، وابتزازهم، باستغلال ضعف الإدراك لديهم، وعدم قدرتهم على التمييز، ما يجعل ابتزازهم والتغرير 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 . 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.
- ضرورة معاقبة كل من الحالات التالية:

دخل من دون تصريح إلى موقع، أو نظام معلومات إلكتروني، أو شبكة معلوماتية، أو وسيلة تقنية معلومات، سواء كان الدخول بقصد الحصول على بيانات حكومية، أو معلومات سرية خاصة بمنشأة مالية، أو تجارية، أو اقتصادية.

كل من دخل من دون تصريح إلى موقع، أو نظام معلومات إلكتروني، أو شبكة معلوماتية، أو وسيلة تقنية معلومات، سواء كان الدخول بقصد الحصول على بيانات حكومية، أو معلومات خاصة بمنشأة مالية، أو تجارية، أو اقتصادية. وتشدد العقوبة إذا تعرضت هذه البيانات أو المعلومات للإلغاء أو الحذف أو الإتلاف أو التدمير أو الإفشاء أو التغيير أو النسخ أو النشر أو إعادة النشر.

يعاقب كل من تحايل على العنوان الإلكتروني باستخدام عنوان وهمي أو عنوان عائد للغير أو بأي وسيلة أخرى، وذلك بقصد ارتكاب جريمة أو الحيلولة دون اكتشافها.

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 معلومات إلكتروني أو إحدى وسائل تقنية المعلومات.

كل من استولى لنفسه أو لغيره بغير حق على أموال أو أوراق مالية أو أي ممتلكات، أو على منفعة اقتصادية أو منقول، أو على سند أو توقيع هذا السند على الشبكة المعلوماتية أو على نظام معلومات إلكتروني أو إحدى وسائل تقنية المعلومات، وذلك بالاستعانة بوسيلة احتيالية إلكترونية تقع باستخدام اسم مستعار أو بطاقة مزورة أو عن طريق سرقة كلمة المرور، أو إدخال لبيانات كمبيوترية أو تعديل أو محو أو حجب للمعلومات والبيانات، أو سرقة هوية المستخدمين من الشبكة، وأي تدخل في عمل نظام الكمبيوتر، أو أنظمة التشغيل والاتصالات أو البرامج أو المواقع الإلكترونية أو محاولة تعطيلها أو تغييرها، بنية احتيالية أو غير مشروعة، أو بالاستعانة بمواقع وهمية أو حقيقية للاستيلاء دون وجه حق لخداع المجني عليه لحمله على تقديم أموال أو أوراق مالية أو أي ممتلكات، أو على منفعة اقتصادية أو منقول أو سند لنفسه أو للغير.

كل من اعتدى على أي من المبادئ أو القيم الأسرية أو نَ أخباراً أو صوراً تتصل بحرمة الحياة الخاصة أو العائلية للأفراد، ولو كانت صحيحة، عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات، كل من اعتدى على أي من المبادئ أو القيم الأسرية أو نشر معلومات أو أخباراً أو صوراً تتصل بحرمة الحياة الخاصة أو العائلية للأفراد، ولو كانت صحيحة، متى ترتب على ذلك ضرر، عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات.

كل من أنشأ أو أدار موقعاً إلكترونياً أو أشرف عليه أو نشر معلومات على شبكة معلوماتية أو بإحدى وسائل تقنية المعلومات، بقصد الاتجار في البشر أو الأعضاء البشرية، أو التعامل فيها بصورة غير مشروعة.

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.

كل من أنشأ أو أدار موقعاً إلكترونياً، أو أشرف عليه أو استخدم معلومات على الشبكة المعلوماتية أو 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.

كل 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.

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.
- د/ زاهر راضي, استخدام مواقع التواصل الاجتماعي في العالم العربي, مجلة التربية, جامعة عمان الأهلية, 2003.
- د/ مجدي محمد عبد الجواد الداغر, استخدامات الإعلاميين لشبكات التواصل الاجتماعي والإشباعات المتحقق, 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:**

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

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.

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.

- 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.

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-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.

Journal Officiel:

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

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.

-J**ORF** 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 .

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.