مجلّة الواحات للبحوث والدراسات
ردمد-P 7163 – 1112
ردمد-E 1892 – 2588
http://elwahat.univ-ghardaia.dz

سلطات الضبط الإداري في مواجهة المخاطر الأمنية لشبكات التواصل الاجتماعي

آيت عودية بلخير محمد [1]، شول بن شهرة [2،3]
قسم الحقوق و العلوم السياسية – جامعة غرداية
1- باحث دكتوراه ، كلية الحقوق و العلوم السياسية، جامعة باتنة 1
2 - قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة غرداية.
3- رئيس مشروع تكوين دكتوراه : ل. م. د قانون عام اقتصادي ،جامعة غرداية.
aitaoudiabm@gmail.com[1]
djawwal@gmail.com[2]

ملخص:

استحداث شبكات التواصل الاجتماعي و إن كان يهدف بالأساس لتطوير وسائل الاتصال و التقريب بين الناس، إلا أن استخدامها سرعان ما امتد ليشمل العديد من النشاطات الإجرامية التي تهدد أمن المجتمع و نظامه، سواء من خلال استغلال تلك الشبكات كمنصات نشاط و دعم للجماعات الاجرامية، أو من خلال توظيفها في عمليات تحريض الجماهير و بث الشائعات. أمام هذا الواقع، تبرز الحاجة للدور الوقائي الذي تضطلع به أجهزة الضبط الإداري. و التي زودت لهذا الغرض بتدابير تقنية خاصة تعمل وفقا لنظام متكامل؛ حيث يتم وضع نظام يقظة إلكترونية يقوم على تقنية تحليل الشبكات الاجتماعية الالكترونية بهدف الكشف المبكر عن المجموعات و المضامين المخلة بالأمن العام. لتتولى الأجهزة المختصة بعد ذلك، إزالة تلك المحتويات أو ضبط النفاذ إليها في حالة الضرورة.

كلمات مفتاحية -

ضبط إداري - شبكات التواصل الاجتماعي - الأمن العام

Administrative Police In Face Of Social Media Risks On Homeland Security.

Abstract–

Although The Creation Of Social Media Aims To Develop Means Of Communication And Rapprochement Between People, But Its Use Extend To Include Many Criminal Activities That Threaten The Security Of The Society And Its System, Whether By Exploitation Of These Networks As Platforms For Committing Crimes And Supporting Criminal Groups, Or By Using It To Incitement To Violence And Spread Rumors. In View Of This Reality, There Is A Need For The Preventive Role Of The Administrative Police. Which Has Special Technical Measures Operates In An Integrated System; An Electronic Patrol Based On Online Social Network Analysis Developed To Detect Criminal Groups And Harmful Contents. The Competent Authorities Shall Then Precede To Remove Those Contents Or, If Necessary, Block The Access To All The Website.

Keywords-

Administrative Police - Social Media - Homeland Security.

مقدمة –

بالرغم من أن استحداث شبكات التواصل الاجتماعي كان يهدف بالأساس لتطوير وسائل الاتصال و التقريب بين الناس، إلا أن استخدامها سرعان ما امتد ليشمل العديد من النشاطات الإجرامية التي تصيب أمن المجتمع و نظامه كتشجيع و دعم الإرهاب و الجماعات الإجرامية، أو إثارة الفتن الطائفية و العرقية و نشر الشائعات.

تعرف الجزائر تزايدا لافتا في الإقبال الجماهيري على الشبكات الاجتماعية الإلكترونية، و هو ما ضاعف من خطورة النشاطات الإجرامية المرتبطة بهذا النوع من الشبكات لما في ذلك من توسيع لدائرة الاستهداف و التأثير. فوفقا لإحصائيات الثلاثي الأول من سنة 2017؛ تحتل الجزائر المرتبة الثالثة عربيا من حيث عدد منتسبي شبكة Facebook بنسبة 12٪. مع تسجيل 9.38 مليون

مشترك جديد بين سنتي: 2014 و 2017، لتكون بذلك في المرتبة الثانية من حيث سرعة الزيادة بعد مصر[1]. كما تضم أيضا نسبة 09 ٪ من عدد منتسبي شبكة Twitter في العالم العربي، مع زيادة استثنائية عرفتها الفترة الممتدة ما بين: 2014 و 2016 بلغت 773500 مشترك جديد بنسبة 2603 ٪، لتتحل بذلك المرتبة الأولى عربيا من حيث الزيادة في هذه الفترة[2]. هذه الزيادات أدت بدورها إلى ارتفاع في عدد الجرائم التي تعالجها مصالح مكافحة الجريمة الإلكترونية و المتعلقة أساسا بالوسائط الإلكترونية للتشبيك الاجتماعي. فبعد معالجتها سنة 2014 لحوالي 211 جريمة تورط فيها 205 شخص[3]، سجلت نفس المصالح في سنة 2016 زيادة معتبرة بـ 567 قضية تورط فيها 543 شخص[4].

يستنهض هذا الواقع العديد من الأدوار القانونية، سواء لدى: المشرع، الإدارة، القضاء أو سلطات الضبط القضائي. لكن من بين أهم هذه الأدوار يبرز بشكل خاص الجهد الوقائي الذي تضطلع به سلطات الضبط الإداري للحد من انتشار هذه النشاطات الإجرامية بشكل مسبق عن وقوعها. من خلال هذه الدراسة نركز على التحدي الذي تفرضه شبكات التواصل الاجتماعي على وظيفة الضبط الإداري في الحفاظ على الأمن العام. إذ أن أجهزة الضبط الإداري تجد نفسها في هذه الحالة في فضاء جديد يختلف عن الفضاء التقليدي الذي اعتادت النشاط فيه، فشبكات التواصل الاجتماعي تتسم بطابعها الجماهيري و اللامادي و العابر للحدود الوطنية. من أجل مناقشة على هذه الإشكالية؛ نبرز في البداية أهم المخاطر الأمنية لشبكات التواصل الاجتماعي (1). لنتطرق عقب ذلك، لأهم التدابير الوقائية التي تملكها سلطات الضبط الإداري لمواجهة تلك المخاطر (2).

1- المخاطر الأمنية لشبكات التواصل الاجتماعي

غدت شبكات التواصل الاجتماعي فضاء مفضلا للعديد من النشاطات الإجرامية التي تهدد الأمن العام، مستفيدة من فعالية تلك الشبكات في الاتصال و من طابعها الجماهيري، بما يخدم توسيع دائرة الاستهداف و زيادة قوة التأثير. من أكثر المخاطر الأمنية التي يمكن أن تنطوي عليها الشبكات الاجتماعية هو استغلالها من طرف الجماعات الإجرامية كمنصة نشاط و دعم

(1- 1)، بالإضافة لاستغلالها من قبل أطراف معادية للتلاعب بالجماهير في إطار ما يسمى بالقوة الناعمة (1- 2).

1- 1- استغلال شبكات التواصل الاجتماعي كمنصات نشاط و دعم للجماعات الاجرامية

الإمكانيات الكبيرة التي تتيحها الشبكات الاجتماعية الإلكترونية للاتصال الشخصي و الجماهيري، سرعان ما تم استغلالها من طرف التنظيمات الإجرامية، لاسيما الإرهابية منها، لتوسيع نطاق تأثيرها و لتطوير مستوى تنظيمي أعلى. و من بين أخطر تلك الاستخدامات يمكن ذكر ما يلي:

أ- التجنيد: تساعد مواقع التواصل الاجتماعي بفعالية على استقدام عناصر جديدة للمنظمات الإجرامية. إذ يمكن لهذه المنظمات أن تحدد المستخدمين الزائرين لصفحاتها و الذين يُبدون تعاطفا أو اهتماما بنشاطاتها (تعليقات، إعجاب، إعادة تغريد...)، لتقوم بعد ذلك بالاتصال بهم لغرض التجنيد[5].

ب- الدعاية: أضحت مواقع التواصل الاجتماعي تستغل بشكل متزايد من طرف المنظمات الإجرامية كمنصات للتواصل و للإعلام، نظرا لمنحها قدرة على التحكم المباشر في مضمون الرسائل و في شكلها (رسائل مكتوبة، صور، فيديوهات، أناشيد...)، و نظرا لتعدد أوجه استخداماتها (ترويج مواد ممنوعة، جلب التعاطف، إرهاب الأعداء و الخصوم، تبني الجرائم، نشر الأفكار و الايديولوجيات، التحريض...)[6].

ج- التدريب و التلقين: يمكن لمواقع التواصل الاجتماعي أن تشكل وسيلة تعليم إلكتروني بيد الجماعات الإجرامية تغنيها عن التدريب و التلقين التقليديين. سواء من الناحية العسكرية أو شبه العسكرية (صنع متفجرات أو أسلحة، تقنيات القتال و استعمال السلاح، أساليب إخفاء المسروقات و تهريب الأشياء المحظورة...)، أو من الناحية الإيديولوجية و الفكرية (تلقين الأفكار المتطرفة، التأسيس للفلسفة و الايديولوجية التي تقوم عليها العصابة، تبليغ الفتاوى المتطرفة...)[7].

د- التمويل: يمكن للشبكات الاجتماعية الإلكترونية أن تستخدم أيضا كوسيلة لتمويل نشاطات العصابات الإجرامية سواء بشكل مباشر كطلب الدعم المالي أو بيع منتجات، أو بشكل غير مباشر عن طريق الابتزاز[8].

1- 2- استغلال الشبكات الاجتماعية الإلكترونية في التأثير على الجماهير

يمكن تصور الجماهير كتكتل من البشر يمتلك خصائص جديدة و مختلفة جدا عن خصائص كل فرد يشكله، و فيه تنطمس الشخصية الواعية للفرد، و تصبح أفكار الوحدات المصغرة المشكلة للجمهور موجهة نحو اتجاه موحد، لتُكوّن كينونة واحدة خاضعة لما يسمى "بقانون الوحدة العقلية للجماهير". و لا يشترط لتحقق الوحدة العقلية للجمهور التواجد المكاني للأفراد، بل المهم الاجتماع على فكرة محددة[9]. و بحسب عالم الأنتروبولوجيا الفرنسي Gustave Le Bon فإن الجماهير تتميز بكونها من الناحية العقلية و الفكرية أقل من الفرد، لكن أكثر منه من الناحية العاطفية و الانفعالية[10]، فمن أبرز خصائص الجمهور حسبه: "سرعة الانفعال و النزق و العجز عن المحاكمة العقلية و انعدام الرأي الشخصي و الروح النقدية و المبالغة في العواطف و المشاعر"[11]. هذه الخصائص تجعل من الجماهير عرضة للانزلاق نحو ارتكاب أفعال العنف الجماعي التي قد تخل بالنظام العام[12].

الشبكات الاجتماعية الإلكترونية كفضاء إعلام اجتماعي تفاعلي تتميز بقدرة هائلة على خلق "وحدة عقلية" بين عدد كبير من الأشخاص لصالح قضايا نبيلة كثيرة، و لكن يمكن أيضا استعمالها بنفس القدر لبث أفكار هدامة تحدث اختلالات أمنية جسيمة، خاصة و أن أكثر رواد الشبكات الاجتماعية هم من فئة المراهقين و الشباب، مما يسهل إغرائهم و إغوائهم لصالح أشخاص، منظمات، أو أجهزة دول لها أهداف تخريبية. حيث يمكن أن توظف هذه القدرة للتحريض على التجمهر و على جرائم ضد أنظمة الحكم و سلطة الدولة. فقد أظهرت العديد من الأحداث الحاصلة في العقد الأخير أن الشبكات الاجتماعية الإلكترونية يمكن أن تلعب دورا مهما في إثارة وتحريض الجماهير بالصورة و الكلمة. و لعل المثال الأبرز على ذلك هو الدور الذي لعبته هذه الشبكات في

أحداث ما سمي "بالربيع العربي". من جهة أخرى، يلاحظ أن لنشر الاشاعات و الأخبار الكاذبة تداعيات خطيرة على الأمن القومي. فالإشاعة يمكن أن تساهم في تمزيق عناصر القوة و الوحدة لأي أمة، من خلال زرع الشكوك و الرعب و الهزيمة في أوساطها، و تدمير القوى المعنوية و تفتيتها، و بث الشقاق و العداء و عدم الثقة و افتعال الكوارث و الأزمات و المشكلات و الأكاذيب، مما يجعل المرء إزاءها في حيرة بين التصديق و التكذيب[13]. فقد اعتبر حلف شمال الأطلسي أن مثل هذه الشبكات يمكن أن تتحول إلى سلاح ضمن إستراتيجيات "الحروب الهجينة"، إذا ما تم استغلالها في شن هجمات إلكترونية اجتماعية تعتمد على "عمليات متعمدة و منظمة لنشر الشائعات و المغالطات و رسائل التلاعب في البيئة الافتراضية بهدف زيادة الخوف و الذعر بين الجماهير"[14].

2- تدابير للوقاية من المخاطر الأمنية لشبكات التواصل الاجتماعي

فضلا عن التدابير اللائحية؛ قد تتدخل سلطات الضبط الإداري بتدابير أخرى مادية من أجل الحد من المخاطر الأمنية لشبكات التواصل الاجتماعي. وتتميز التدابير غير اللائحية في هذا المجال بطابع تقني غالب. حيث يتم وضع نظام يقظة إلكترونية بهدف اكتشاف المضامين المحظورة و الأنشطة الخطيرة بصفة مبكرة (2- 1). لتعمل الأجهزة المختصة عند الاقتضاء بضبط النفاذ إلى الشبكات المعنية، أو ضبط المحتويات المخلة بالأمن العام فيها (2- 2).

2- 1- اليقظة الإلكترونية للوقاية من المخاطر الأمنية لشبكات التواصل الاجتماعي

ترتبط فعالية الدور الوقائي لهيئات الضبط الإداري إلى حد بعيد بتدبير "دوريات المراقبة"، الذي يساعد على توقي أو استشراف الاختلالات التي قد تصيب النظام العام، أو الكشف المبكر عنها لمنع تفاقمها. المرسوم الرئاسي رقم 261- 15 الذي يحدد تشكيلة و تنظيم و كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها، ينيط صراحة بالهيئة وظيفة "اليقظة الإلكترونية"، و ينشئ لذلك مديرية خاصة تدعى "مديرية المراقبة الوقائية و اليقظة الإلكترونية"، و التي تكلف خصوصا بتنفيذ عمليات المراقبة الوقائية للاتصالات الإلكترونية من أجل الكشف عن الجرائم المتصلة

بتكنولوجيات الإعلام و الاتصال[15]. لاسيما تلك المخلة بالنظام العام، مثل الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة، أو الاعتداء على منظومات معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني[16].

نظرا لتعدد مواقع التواصل الاجتماعي و للكثافة العالية لمضامينها و تعقيد التواصل عبرها، لا يمكن الاعتماد في عملية مراقبتها المستمرة على التصفح التقليدي لحساباتها و صفحاتها. بل لا بد من انتهاج أسلوب علمي دقيق يُمكّن من مسح أكبر قدر من المعطيات المفتوحة و يحولها إلى معلومات قابلة للاستغلال في مجال الضبط الإداري. و الأداة المثلى لتحقيق هذه الغاية، تتمثل في تقنية تحليل الشبكات الاجتماعية الإلكترونية، التي تعمل على مستويات مختلفة تشمل كل من هيكلية الشبكة، بياناتها و التفاعل بين عناصرها. و لبيان كيفية ذلك، نركز فيما يلي على تطبيق هذه التقنية في كل من: كشف الجماعات الإجرامية (أ)، و استشراف أعمال الشغب (ب).

أ- تطبيق تحليل الشبكات الاجتماعية الالكترونية لكشف الجماعات الاجرامية

النجاعة العالية لاستخدام شبكات التواصل الاجتماعي من طرف المنظمات الإجرامية في أكثر من صعيد (مثل: التجنيد، الدعاية، التلقين، و التمويل)، يجب أن تقابلها يقظة مستمرة من الجهات الأمنية المختصة بغرض الكشف المبكر و رصد نشاط تلك المنظمات. يساهم تحليل الشبكات الاجتماعية الإلكترونية في كشف الجماعات الإجرامية الخفية على مواقع التواصل الاجتماعي من خلال في عملية تمر بمرحلتين أساسيتين: في مرحلة أولى، يتم تحليل بيانات الشبكة وفقا لمقياس "تحديد الآراء" بواسطة قائمة كلمات مفتاحية تدل على الاستعمالات الإجرامية لمواقع التواصل الاجتماعي و وضع معامل أهمية لكل كلمة لزيادة دقة النتائج. بعد ضبط قائمة الكلمات المفتاحية المناسبة، يتم تفعيل البحث عنها في مختلف مضامين شبكة التواصل الاجتماعي (فيديوهات، تعليقات، تغريدات، رسائل...). لتنتهي هذه المرحلة، بتحديد الحسابات و الصفحات التي تصدر منها تلك النشاطات[17]. في المرحلة الثانية،

يتم تحليل هيكلي للشبكة الاجتماعية الإلكترونية بهدف معرفة العلاقات و التفاعلات التي قد توجد بين مختلف تلك الحسابات. من الناحية البيانية يتمثل المستخدمين في شكل عُقد و تستخرج العلاقات لتمثل في شكل روابط. في الأخير، تتم الاستعانة بعدد من المقاييس الأخرى من أجل فهم أدق لبنية الشبكة و طبيعة العلاقات فيها، كاستعمال مقياس"قوة الروابط" للتميز بين المستخدمين المقربين و النشطين في الشبكة، مقارنة بالمستخدمين الثانويين أو العابرين.

ب- تطبيق تحليل الشبكات الاجتماعية الإلكترونية في استشراف أعمال الشغب

عمليا يمكن أن تساهم كل مستويات تحليل الشبكات الاجتماعية الإلكترونية في الوقاية من التهديدات الجماهيرية التي قد تلحق بالنظام العام. فالتحليل الدلالي للبيانات يساعد على الرصد المبكر لتنامي المشاعر السلبية و تحديد ما إذا كانت ستقتصر على التعبير عن الغضب و الامتعاض، أم أنها ستتطور نحو احتجاجات و شغب على أرض الواقع. أما التحليل الهيكلي وفقا لمقياس المركزية، فيمكّن من التنبؤ بمدى انتشار المضامين و سرعتها من خلال كشف العناصر التي تتمتع بدرجة مركزية عالية في الشبكة و التي تلعب دورا هاما في وصول المضامين لأكبر عدد من المستخدمين. و أخيرا، يؤدي تحليل تفاعلات المستخدمين من معرفة تأثير المضامين و مدى جماهيرية الأحداث المتوقعة. يعتبر "برنامج استخدام البدائل القائم على نموذج التنبؤ المبكر بالأحداث" (E.M.B.E.R.S)، من بين أهم البرامج التي تستفيد من بيانات الشبكات الاجتماعية الإلكترونية في إطار الاستعلام الاستباقي عن الأحداث، و الذي تشرف عليه إحدى الوكالات التابعة لمكتب مدير الاستخبارات الوطنية في الولايات المتحدة الأمريكية[18].

2- 2- ضبط النفاذ إلى شبكات التواصل الاجتماعي و ضبط محتوياتها

لمواجهة بعض التهديدات الجدية للأمن العام، قد تلجأ الضبطية الإدارية لتقييد النفاذ إلى شبكات تواصل اجتماعي محددة، عبر تفعيل آليات معينة

في البنية التحتية للإنترنت في الدولة (أ). كما قد يتم اللجوء لإجراء أقل صرامة نسبيا في مواجهة بعض المحتويات المخلة بالنظام العام، حيث تعمل الأجهزة المختصة على حجبها عن نطاق جغرافي معين، أو تطلب إزالتها كليا من الشبكة (ب).

أ- ضبط النفاذ إلى مواقع شبكات التواصل الاجتماعي

يعتبر ضبط النفاذ أو "الحجب" من التدابير الوقائية المانعة لممارسة النشاط. و في إطار الضبط الإداري، يقصد بحجب مواقع الشبكات الاجتماعية الإلكترونية؛ إجراء تقوم به الأجهزة المختصة بمساعدة مقدمي الخدمات الوسيطة عادة، تمنع من خلاله المستخدمين في نطاق جغرافي معين (مثل: دولة، إقليم، مقاطعة)، من الوصول إلى موقع أو أكثر من مواقع شبكات التواصل الاجتماعي، بصفة دائمة أو مؤقتة، من أجل حماية أو إحلال النظام العام بمختلف عناصره[19].

بالرغم من عدم سن المشرع الجزائري، إلى غاية الحين، نظام قانونيا واضحا و موحدا يحكم عملية حجب المواقع من حيث جهة الاختصاص، حالات الحجب، الإجراءات و الضمانات، إلا أن الجزائر تملك منظومة قانونية و تقنية تسمح لها بحجب مختلف المواقع بما فيها تلك المخصصة للتواصل الاجتماعي الشبكي. فالقانون رقم 09- 04 الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها، يقضي في المادة 12 منه بأنه يتعين على مقدمي خدمات الإنترنت وضع ترتيبات تقنية تسمح بحصر إمكانية الدخول إلى الموزعات التي تحتوي معلومات مخالفة للنظام العام.

ب- ضبط المحتوى المخل بالأمن العام في شبكات التواصل الاجتماعي

خلافا لتدبير حجب المواقع الذي يؤدي لمنع الوصول إلى الشبكة الاجتماعية الإلكترونية في منطقة محددة، فإن تدبير ضبط المحتوى يقتصر فقط على إزالة المحتوى المخل بالأمن العام، دون حظر الوصول إلى الشبكة ككل. كما أن هذا التدبير يتميز بفعالية بالغة في مكافحة المضامين المخلة بالنظام العام إذا كانت محددة و محدودة. لكن تلك الفعالية تتأثر بصفة كبيرة بعنصر الزمن. فكلما تأخر تفعليه، زادت احتمالية انتشار المحتوى بين المستخدمين و انتقاله إلى

شبكات اجتماعية أخرى، مما يصعب من إمكانية ضبطه. هذا الأمر يفترض استجابة سريعة من طرف مواقع الشبكات الاجتماعية الالكترونية - لاسيما تلك الواقعة في الخارج- لإخطارات سلطات الضبط الإداري في الدول، و هذا ما لا يتم دائما نظرا للسلطة التقديرية الواسعة التي تمنحها تلك المواقع لنفسها، و نظرا لغياب آليات إلزامها في العديد من القوانين الداخلية الدول. ففي الجزائر مثلا، و بالرغم من إلزام مقدمي الخدمات الوسيطة بموجب الفقرة الأولى من المادة 12 من القانون 09- 04 بـ: "التدخل الفوري لسحب المحتويات التي يتيحون الاطلاع عليها بمجرد العلم بها بطريقة مباشرة أو غير مباشرة بمخالفتها للقوانين و تخزينها أو جعل الدخول إليها غير ممكن". إلا أن هذا النص لا يُلزم عمليا إلا أولئك الخاضعين للقانون الجزائري، و لا يمكن أن يساهم بنجاعة في إلزام مواقع الشبكات الاجتماعية الإلكترونية الواقع بالخارج للاستجابة لطالبات أجهزة الضبط الإداري لإزالة محتوى مخل بالنظام العام في البلد.

خاتمة

إجابة على إشكالية الدراسة و على ضوء ما سبق، وجدنا أن الطابع الجماهيري و الفوق وطني لشبكات التواصل الاجتماعي يمكن أن يوظف بشكل سلبي من طرف عناصر أو مجموعات إجرامية أو منظمات بهدف المساس بأمن المجتمعات. أمام هذا الواقع تبرز أهمية الدور الوقائي الذي تضطلع به أجهزة الضبط الإداري، التي تتمتع، فضلا عن التدابير اللائحية، بتدابير تقنية تعمل وفقا لنظام متكامل. حيث يتم وضع نظام يقظة إلكترونية بهدف تسيير دوريات لاكتشاف المضامين المهددة للأمن العام بصفة مبكرة. لتعمل الأجهزة المختصة بعد ذلك، على إزالة تلك المحتويات أو ضبط النفاذ إليها عند الاقتضاء. مع تسجيل محدودية فعالية النظام القانوني النافذ في الجزائر في حالة عدم تعاون مقدمي الخدمات الوسيطة في الخارج.

الهوامش

[1] -Salem, F., The Arab Social Media Report 2017: Social Media and the Internet of Things: Towards Data-Driven Policymaking in the Arab World (Vol. 7). Dubai: MBR School of Government, 2017, p. 37.

[2] -Ibidem, pp. 45-46

[3]- http://www.algeriepolice.dz/? مصالح- شرطة- مكافحة-الجرائم- الإلكترونية- تسجل (Consulté le 23/09/2017)

[4] - http://www.algeriepolice.dz/? الأمن- الوطني- يعالج،4800 (Consulté le 23/09/2017)

[5] - Lord Carlile QC, Stuart Macdonald, The Criminalisation of Terrorists' Online Preparatory Acts, in Thomas M. Chen et al. (eds.), Cyberterrorism: Understanding, Assessment, and Response, Springer Science+Business Media, New York, 2014, p. 159.

[6] - Ibidem; David Décary-Hétu & Carlo Morselli, Gang Presence in Social Network Sites, International Journal of Cyber Criminology (IJCC), December 2011, Vol 5 (2), p. 880.

[7]- أسماء الجيوشي مختار، دور استخدام التنظيمات الارهابية لمواقع التواصل الاجتماعي في اقناع الأفراد بأفكارها، الندوة العلمية حول دور مؤسسات المجتمع المدني في التصدي للإرهاب. 26- 2014/08/28، الجزائر، ص 81 و ما بعدها. مداخلة متوفرة على الرابط: http://repository.nauss.edu.sa/handle/123456789/57651 (تاريخ الاطلاع: 2017/05/08).

[8] - Lord Carlile QC, Stuart Macdonald, op.cit, p. 160.

[9]- محمد علي فرح، صناعة الواقع: الاعلام و ضبط المجتمع، الطبعة الأولى، مركز نماء للبحوث و الدراسات، بيروت، 2014، ص 39- 40.

[10]- غوستاف لو بون، سيكولوجية الجماهير، ترجمة: هاشم صالح، الطبعة الأولى، دار الساقي، بيروت، 1991، ص 59.

[11]- المرجع نفسه، ص 63.

[12]- لأكثر تفصيل في هذا الشأن يمكن الرجوع إلى: حسين بن ابراهيم ياسين الحلوي، جرائم العنف الجماعي، رسالة ماجستير، قسم العدالة الجنائية، جامعة نايف العربية للعلوم الأمنية، الرياض، 2010، ص 72 و ما بعدها.

[13]- تريكي حسان، مرجع سابق، ص 198.

[14]- Anna Reynolds (ed.),Public Report social media as a tool of hybrid warfare, NATO StratCom COE Riga, May 2016, p 18. Available at: https://www.stratcomcoe.org/download/file/fid/5314 (Accessed 04/09/2017).

[15]- المادة 11 من المرسوم رئاسي رقم 261- 15 الذي يحدد تشكيلة و تنظيم و كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها.

[16]- المادة 04 من القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها.

[17] - I-Hsien Ting et al., An Approach for Hate Groups Detection in Facebook, in: L. Uden et al. (eds.), The 3rd International Workshop on Intelligent Data Analysis and Management, Springer Proceedings in Complexity, Springer Science+Business Media Dordrecht, 2013, p 102.

[18] - Andy Doyle et al., The EMBERS Architecture for Streaming Predictive Analytics, In: International Conference on Big Data, IEEE Computer Society Washington, DC, USA, 2014, pp. 11-12.

[19] - Conseil de l'Europe, l'Étude comparative sur le blocage, le filtrage et le retrait de contenus illegaux sur internet, Lausanne, 2017, pp. 03-04.