نهاية الخصوصية:
الحريات الشخصية وأمن الدول في عصر البيانات الضخمة

نور سلمان
باحث متخصص في الدراسات الإعلامية والثقافية

أحدثت شبكات التواصل الاجتماعي ثنائية متناقضة تماماً فيما يخص حريات الأفراد على المستوى العالمي؛ ففي الوقت الذي أضحى فيه الفرد أكثر حرية في التعبير عن رأيه، ربما بدون حدود، فإنه يتعرض في المقابل إلى مختلف المخاطر فيما يتعلق بخصوصيته الذاتية، بما قد يهدد حرياته وخياراته المفترضة في كثير من الأحوال.

ويعزى ذلك إلى زيادة أنماط التفاعل بين المجتمعات وانسيابية وسيولة البيانات الضخمة (Big Data)، وذلك في الوقت الذي تزداد فيه الرقابة بصورة كبيرة، ارتباطاً بالتطور في تكنولوجيا المعلومات، وزيادة استخدام الأجهزة الذكية والإنترنت، كما ظهر جلياً منذ قيام إدوارد سنودن بإفشاء وثائق وكالة الأمن القومي الأمريكية في عام 2013، والتي كشفت عن قيام الولايات المتحدة بمراقبة البيانات الضخمة، ليثير ذلك جدلاً كبيراً حول الخصوصية، على المستويات المحلية والإقليمية والدولية.

في هذا الإطار تناقش هذه الورقة بعض الممارسات التي اتبعتها الحكومات واللاعبون التجاريون لمراقبة البيانات الضخمة، والتداعيات السلبية المترتبة على ذلك فيما يرتبط بالخصوصية، لاسيما في سياق انتشار التقنيات التفاعلية الجديدة وزيادة استخدام مواقع التواصل الاجتماعي، وهو الأمر الذي يثير العديد من الأسئلة مثل: كيف يقوم التقدم التكنولوجي والمراقبة بالقضاء على الخصوصية في عصر العولمة؟ وهل يكون استخدام الرقابة والبيانات الضخمة جزءاً من استراتيجية مكافحة الإرهاب؟ وأين تنتهي حدود الخصوصية؟ وهل يمكن اعتبار استخدام البيانات الضخمة نهاية للحريات المدنية؟

أولاً: التواصل الاجتماعي ومفارقة الخصوصية

تمثل مواقع التواصل الاجتماعي "مناخاً اجتماعياً فريداً" ضمن نطاق الجيل الثاني من شبكة الإنترنت (Web 2.0)[1]، ويجري استخدام هذه المواقع، ومنها فيسبوك، وتويتر، وورد برس، ويوتيوب، وفليكر، ولينكد إن، وتمبلر؛ لإيجاد وإدامة الروابط الاجتماعية وذلك بواسطة جمع كميات كبيرة من المعلومات الشخصية[2]، إذ يمكن ذلك الأفراد، بشكل غير مسبوق، من التواصل والتعبير عن آرائهم من خلال تحميل الصور والفيديوهات ومشاركة الروابط الخاصة عبرها، والتعبير شخصياً عن الذات والآراء، وأحياناً الحالة الشخصية من خلال مواقع التواصل والمدونات، بل ويسعى الأفراد إلى الحفاظ على تواجدهم في هذه المجتمعات المصغرة التي تشكلت من خلال الإنترنت.

وتذهب الدكتورة لوشيا تللو دياز – الباحثة بقسم الصحافة، كلية علوم الإعلام في جامعة كومبلوتنس

في مدريد – للقول إن البيانات المجمّعة من الحسابات الشخصية (Profiles) على مواقع التواصل الاجتماعي تمثّل في الأصل وثيقة هوية، تتعلق المعلومات المتوفرة من خلالها "بالخصوصية الشخصية"، ولذا فهي بالضرورة "معلومات سرّية"[3]. ولأن خصوصية الفرد ضمن عالم مواقع التواصل الاجتماعي تدور حول ماهية المعلومات التي يتم التشارك بها وكذلك حول الغرض من هذا التشارك[4]؛ فإن السؤال هنا: كم من هذه المعلومات يعتبر خصوصياً بالفعل إذا أخذنا بعين الاعتبار مثلاً شبكة العلاقات الاجتماعية التي يقدمها فيسبوك (Facebook Social Graph)، الذي يمثل أكبر مجموعة بيانات في العالم تقوم برسم شبكة العلاقات بين مختلف المستخدمين، وإظهار كيفية ارتباط بعضهم بالبعض الآخر[5].

وبحسب دراسة حديثة أجراها مركز بيو للبحوث (Pew Research Center)، فإن معظم البالغين الذين شملتهم الدراسة "يشعرون بأن الخصوصية تتعرض للانتهاك في أبعاد جوهرية مثل أمن المعلومات الشخصية وقدرتهم على الاحتفاظ بالخصوصية"[6]، وهنا يبرز ما يمكن تسميته "الانقسام المضاعف" (Double dichotomy) أو مفارقة الخصوصية (Privacy paradox)، والتي يمكن تعريفها على أنها "التنافر بين رغبة ونيّة الفرد في مشاركة معلوماته الشخصية من جهة، وأنماط فضح خصوصيته الفعلية من قبل مواقع التواصل الاجتماعي من جهة أخرى"[7]، وهو ما يثير التساؤل حول الأسباب التي تجعل الأفراد مستعدين لمشاركة كل هذه المعلومات على الرغم من المخاوف من انتهاك الخصوصية، خاصة في حقبة ما بعد تسريبات سنودن؟

تكمن الإجابة في بنية وتصميم مواقع التواصل الاجتماعي، فهما بحكم طبيعتهما، يشجعان المستخدمين على إفشاء كم كبير من البيانات الشخصية أثناء إنشاء أو تحديث صفحات البيانات الشخصية الخاصة بهم، والتي تشمل معلومات من قبل: الاسم الكامل للفرد وتاريخ ميلاده وميوله السياسية[8].

إن أحد أهم العوامل التي تدفع الأفراد لمشاركة معلوماتهم الشخصية هو حصولهم في المقابل على خدمات مجانية من خلال مواقع وتطبيقات التواصل الاجتماعي. وبحسب مشروع الإنترنت الذي يديره مركز بيو للبحوث، تبين أن 62% من الأفراد المشمولين بالمسح كانوا مستعدين لمشاركة بعض المعلومات الشخصية من أجل الحصول على خدمات مجانية عبر الهواتف الذكية والأجهزة اللوحية من دون أن يعرفوا حقاً ما هي المعلومات التي يتم إرسالها إلى الأطراف الثالثة كشركات الإعلانات مثلاً[9]، وما يثير الاهتمام هنا أن 61% ممن شملهم المسح عبّروا عن رغبتهم في اتخاذ إجراءات إضافية من أجل حماية خصوصيتهم ومعلوماتهم الشخصية.

ويعني هذا أنه بدلاً من حماية الخصوصية الشخصية، فإن المستخدمين يكونون أكثر قلقاً حيال من لديه القدرة على الوصول إلى معلوماتهم الشخصية أكثر من قلقهم من الكيفية التي ستقوم بها الشركات والأطراف الثالثة باستخدام معلوماتهم تلك[10].

وما يبدو واضحاً هنا أن المستخدمين سيواصلون نشر معلوماتهم الشخصية عبر مواقع التواصل الاجتماعي ما دام لديهم اعتقاد بأنهم يملكون القدرة على التحكم في خصوصيتهم وحمايتها من خلال إعدادات الخصوصية، لكن المفارقة هنا تتمثل في أن مقدار التحكم (أي قدرة المستخدم على منع المستخدمين الآخرين من الاطلاع على بياناته الشخصية التي يرغب في عدم إظهارها أمامهم) الذي يمتلكه المستخدمون بالفعل يكاد يكون معدوماً فعلياً، إذا أخذنا بعين الاعتبار التطورات السريعة في مجال التكنولوجيا الذكية وطرق المراقبة المتزايدة التي تستخدمها الهيئات الحكومية والشركات على حد سواء، والتي تجعل هذا التحكم المتوهم من قبل الأفراد غير مجدياً لحماية خصوصيتهم.

ثانياً: تطور التكنولوجيا الذكية والمراقبة

تثير الهواتف الذكية والأجهزة اللوحية والتقنيات المتقدمة الأخرى الانتباه إلى مجموعة من المسائل المتعلقة بالخصوصية والمراقبة. ففي منطقة الشرق الأوسط، هناك 56 مليون مستخدم للفيسبوك، و3.7 مليون مستخدم لتويتر، والأغلبية العظمى من هؤلاء يستخدمون تقنيات الهواتف الذكية[11]، وإلى حد بعيد، تساعد مواقع التواصل الاجتماعي والهواتف الذكية وتكنولوجيا المراقبة على التنقيب على البيانات الضخمة، وذلك من خلال "استخدام أساليب إحصائية وبرامج متعددة يمكنها متابعة البيانات الشخصية حتى خلال فترة ماضية[12].

وتستمر عملية تتبع واستخراج البيانات في التوسع، بفضل التقدم في التكنولوجيا، ويشمل ذلك القدرة على تعقب موقع شخص ما، وعلاقاته الشخصية، وتفضيلاته الخاصة، وسلوكياته التجارية، وكل ذلك من خلال هاتفه الذكي، هذا خلافاً للبيانات التي يتم جمعها من الصور الفوتوغرافية التي يتم تحميلها مع إحداثياتها الجغرافية، والتعرف على الوجوه على الفيسبوك وأنستجرام، وكذلك مراقبة البيانات الحسابية[13]، فإذا ما تم أخذ كل ذلك في الحسبان، يكون السؤال المنطقي الذي يحتاج إلى إجابة هو: هل يكون مستخدمو الهواتف الذكية والتقنيات المتقدمة مدركين مدى انتهاك واختراق بياناتهم الشخصية؟

من خلال هذه التقنيات المتقدمة لآليات الرقابة، والتي تسمح بجمع البيانات بسهولة، أمكن المساعدة في اتخاذ إجراءات ذات طبيعة استباقية (مثلاً في مجال مكافحة الإرهاب)، فمن الملحوظ أن الحرب على الإرهاب في مرحلة ما بعد 11 سبتمبر 2001 لعبت دوراً كبيراً في تفعيل أنماط الرقابة الاستباقية، واستغلال الفضاء الإلكتروني من قبل الدول للحد من أو حتى القضاء على الحريات الفردية والخصوصية الشخصية.

أوجد هذا الأمر معه مجتمعاً معلوماتياً يسمح للحكومات وكذلك شركات الطرف الثالث باستخدام طرق المراقبة وتطبيقها بطريقة تجعل "الأشخاص الذين تم جمع أو مراقبة معلوماتهم الشخصية لا يعلمون ما إذا كانوا تحت المراقبة أم لا، ومتى يتم ذلك"[14]، وهو ما انطبق على ملايين الأفراد حول العالم.

ويقول رونالد جيه ديبرت – أستاذ العلوم السياسية ومدير المعهد الكندي للشؤون الأمنية والدولية – إن أكبر منتج ومروّج لبرمجيات الرقابة، خاصة تلك المتعلقة بمراقبة الفضاء الإلكتروني هي بلدان

أمريكا الشمالية وأوروبا، حيث تكون "الأسواق المستهدفة هي مناطق الجنوب والشرق من العالم، والتي تشهد تطوراً تكنولوجياً متسارعاً وزيادة هائلة في استخدام الإنترنت، فضلاً عن سعي الأنظمة الاستبدادية لإدامة سيطرتها ورقابتها على مواطنيها الذين يتأثرون بالأفكار التي يتم الترويج لها من خلال الإنترنت، وأحياناً تدفعهم لاتخاذ خطوات ملموسة في العالم الواقعي،"[15]، على نحو ما شهدته الثورات العربية والأحداث اللاحقة لها.

كل هذا يثير العديد من التساؤلات من قبيل: أين تكون الحدود الأخلاقية بين حق الحكومات في إعمال تقنيات المراقبة لحماية الأفراد من التهديدات المختلفة، وبين الخصوصية الفردية؟ وهل انتهت الحريات المدنية إلى غير رجعة؟ وأين تبدأ مسؤوليات الأفراد والحكومات وشركات الطرف الثالث؟ وأين تنتهي؟ وهل يجري تطبيق تقنيات المراقبة هذه في حالة الأنظمة الاستبدادية وحدها أم الديمقراطية كذلك؟، ومن جهة أخرى، ألا ينبغي على البلدان التي توفر هذه التقنيات أن تخضع للمساءلة؟

على الرغم من أهمية خصوصية الأشخاص وحرياتهم المدنية، فإن الجدل حول المراقبة والخصوصية يقع ضمن ثنائية تكون فيها الخصوصية إما ميتة أو موجودة بالكاد، وتستبعد هذه الثنائية أية إمكانية لحدوث جدل علني بين العامة والحكومة والشركات للبحث عن سبل تعزيز الخصوصية في عصر المعلومات وحقبة البيانات الضخمة.

وعلى الرغم من ذلك، تظهر من فترة لأخرى محاولات للدفاع عن الخصوصية، فعلى سبيل المثال، قامت كبريات الشركات ومنها الفيسبوك وتويتر وجوجل ومايكروسوفت وآبل بتشكيل تحالف تحت مسمى "الإصلاح الشامل للمراقبة الحكومية"، وذلك من أجل دعم إقرار مشروع قانون الحرية في الولايات المتحدة، وذلك على الرغم من أن الشركات المذكورة تورطت في المشروع الخاص ببرنامج المراقبة واستخراج البيانات (PRISM)، الذي تديره وكالة الأمن القومي، والذي كان يتيح تجميع البيانات الشخصية لمستخدمي خدماتها، وذلك وفق ما ورد في تسريبات إدوارد سنودن.

ويقول صموئيل جيبز – المحرر التكنولوجي في جريدة الجارديان البريطانية – إن مشروع قانون الحرية يهدف إلى وقف عملية "استخراج البيانات" من البريد الإلكتروني والبيانات الوصفية (Metadata) الخاصة بالإنترنت، لكنه يرى أن ذلك لن ينفي استمرار شركات التكنولوجيا في الإفصاح عن المعلومات الخاصة بالبيانات التي تطلبها الحكومة، وذلك كجزء من مساعي هذا القطاع في الحفاظ على الشفافية"[16].

ولكن من المهم هنا الإشارة إلى أن مجرد قيام عمالقة التكنولوجيا والتواصل الاجتماعي بمحاولات تعزيز الشفافية لا يعني بالضرورة أن عملية استخراج البيانات الضخمة والمراقبة ستنتهي، خاصة مع إشارة تقارير صحفية – تم الكشف عنها أوائل عام 2014 – إلى قيام هذه الشركات العملاقة بتسليم عشرات الآلاف من قواعد البيانات الخاصة بعملائها كل ستة أشهر إلى السلطات الحكومية الأمريكية[17].

ثالثاً: البيانات الضخمة وعشوائية الرقابة

في يونيو 2013، قام إدوارد سنودن بتسريب وثائق سرية للغاية إلى صحيفة الجارديان البريطانية وصحيفة واشنطن بوست الأمريكية، وفيها كشف النقاب عن أن وكالة الأمن القومي الأمريكية تقوم، وعلى نحو عشوائي، بجمع سجلات الاتصالات الهاتفية الخاصة بملايين المواطنين الأمريكيين ضمن مختلف الولايات. وما زاد من شدة الصخب الذي أثارته تسريبات سنودن هو كشفها عن أن الوكالات والهيئات الفيدرالية الأمريكية تتمتع، بموجب برنامج بريزم (PRISM)، بإمكانية الوصول إلى الحواسب الخادمة لكبريات شركات التكنولوجيا بما فيها مايكروسوفت وآبل وجوجل وفيسبوك وياهو وسكايب[18]، وأنكر عدد كبير من هذه الشركات في بادئ الأمر هذه المزاعم المتعلقة بالبرنامج، لكن، وكما ذكرنا آنفاً، قامت هذه الشركات بتسليم وسائل التحكم في الخصوصية والتشفير بنفسها للحكومة الأمريكية.

وكشفت ملفات سنودن عن أن مهمة وكالة الأمن القومي لا تركز فقط على استخدام آليات المراقبة لجمع البيانات على مستوى العالم، بل تركز أيضاً على المراقبة وجمع البيانات على المستوى المحلي كاستراتيجية استباقية مضادة للإرهاب، وثارت إثر ذلك الحدث ضجة إعلامية وشعبية مصحوبة بمشاعر الاستياء وانعدام شعور المواطنين بالأمن ضمن الولايات التي يعيشون فيها، فأين يكمن التوازن بين تأمين مصالح الأمن القومي وحقوق المواطن الفردية؟

> **وضعت تسريبات إدوارد سنودن البذور الأولى لقضيتي الانتهاك الواضح للخصوصية والغضب والخوف وانعدام الشعور بالأمن في نفوس المستخدمين لمواقع التوصل الاجتماعي، ومفهوم السيادة في الفضاء الإلكتروني. والنتيجة أن التوازن بين صيانة الحريات المدنية ومصالح أمن الدولة يشهد اختلالاً متزايداً لصالح أمن الدولة؛ ليقوض ذلك الخصوصية في عصر البيانات الضخمة بفعل الممارسات الفردية وممارسات الشركات في عصر العولمة.**

هنا يجادل المشرعون في أن الإجراءات القانونية القائمة جيدة، خاصة أن هناك تناسباً ما بين إجراءات المراقبة والحريات المدنية، كما أن هناك حجة أخرى تلقي اللوم على دور وسائل الإعلام السلبي، وكيف أن الطريقة التي من خلالها الكشف عن معلومات حساسة كهذه – كما هي الحال في ملفات سنودن – يمكن أن تلحق الضرر بأمن الدولة[19]،

وتتجاهل وجهة النظر السالف ذكرها المخاطر التي تتعرض لها الحريات المدنية، لاسيما مع عدم اتخاذ إجراءات فاعلة، أو سن تشريعات من أجل تنظيم التطبيق الاستباقي لبرامج الرقابة. ويقول دافيد لوي – المحاضر بكلية الحقوق، جامعة ليفربول جون مورز – "إن الأمن والحرية يمثلان مصالح حيوية لا يجوز الانتقاص منها، فلا ينبغي تقويض حرية الفرد من خلال إصدار تشريعات تعالج الإرهاب"[20]. فإذا وضعنا نصب أعيننا هذه الشمولية، يصير التساؤل: ما هي التحديات التي يفرضها الفضاء الإلكتروني

فيما يتعلق بحوكمة الإنترنت، ومن هو المسؤول هنا؟

ويمكن القول هنا إن الولايات المتحدة تتحكم في الإنترنت، وذلك في ضوء تحكمها بمفردها في السياسات المرتبطة بحرية الإنترنت وحقوق الملكية الفكرية ومراقبة البيانات الضخمة"[21]، وذلك من خلال منظمة الآيكان (ICANN)، وهي المجموعة المسؤولة عن الحفاظ على معايير عناوين وأسماء النطاقات على شبكة الإنترنت، وهي تخضع للقوانين الأمريكية ولوزارة التجارة الأمريكية، غير أن دورها لا يقتصر على الجانب التقني، بل تقوم بصياغة السياسات حول عدد من المسائل أبرزها حقوق الملكية الفكرية وقضايا الخصوصية وأمن الفضاء الإلكتروني؛ وبالتالي فهي تضع سياسات تدخل في نطاق سيادة الدول الأخرى، ولذلك يجب أن تكون حوكمة الإنترنت متعددة الجوانب وديمقراطية وشفافة، ولكن نظراً لأن مجلس الشيوخ الأمريكي يقوم بتعطيل إقرار مشروع "قانون الحرية" الذي سبقت الإشارة إليه، فإن الجواب يبقى مجهولاً[22].

خاتمة

لقد نال الجدل حول "نهاية الخصوصية" نصيبه الوافي من البحث، وعلى الرغم من ذلك ليس هناك جواب نهائي وحاسم فيما يتعلق بخصوصية الفرد ونهاية حرياته المدنية، والغريب أنه في حقبة ما بعد تسريبات سنودن، لايزال مستخدمو مواقع التواصل الاجتماعي مستعدين لتقديم معلوماتهم الشخصية إلى أطراف ثالثة من دون أن يعلموا حقاً كيف سيتم استخدام هذه المعلومات.

إن مفارقة الخصوصية هذه هي ما تسبب في استمرار الجدل حولها، خصوصاً في سياق التساؤل عن الجهة التي تتحكم في المعلومات، سواءً في شكلها الشخصي أم المؤسسي. ويستمر الحديث عن الخصوصية مثاراً كذلك بسبب النمو الهائل والمتسارع في قدرات الدول على تطوير برامج للمراقبة والبحث، لاسيما مع التقدم التكنولوجي المتسارع، خاصة في ضوء قيام الديمقراطيات بتمويل وبيع هذه البرامج.

لقد قام سنودن بتسريب ما هو أكثر من مجرد استغلال وكالة الأمن القومي، وبمساعدة مواقع التواصل الاجتماعي، لعملية جمع البيانات الضخمة كي تقوم برسم خرائط العلاقات والارتباطات الاجتماعية لمستخدمي هذه المواقع في محاولة لاستباق النشاطات الإرهابية. لكن ذلك وضع البذور الأولى للانتهاك الواضح للخصوصية والغضب والخوف وانعدام الشعور بالأمن في نفوس المستخدمين لهذه المواقع، كما أن تسريبات سنودن فتحت أيضاً جدلاً آخر حول حوكمة الإنترنت والطريقة التي يتم بها تطبيق مفهوم السيادة في الفضاء الإلكتروني، خاصة أن التوازن بين صيانة الحريات المدنية ومصالح أمن الدولة يشهد اختلالاً متزايداً لصالح أمن الدولة؛ فالمراقبة التي تمارسها الدول ستواصل توسعها ونموها، وعلى الرغم من أن الخصوصية لم تمت، فمن المؤكد أنه تم تقويضها بفعل الممارسات الفردية وممارسات الشركات في عصر العولمة.

1- Alyson Leigh Young and Anabel Quan-Haase, “Privacy Protection Strategies on Facebook”, **Information, Communication & Society,** Vol. 16, no. 4, 2013, p. 480.
2- Helen Nissenbaum, **Privacy in Context: Technology, Policy, and the Integrity of Social Life**, (USA: Stanford University Press, 2010), p. 59.
3- Lucía Tello Díaz, “Intimacy and Extimacy in Social Networks. Ethical Boundaries of Facebook”, **Scientific Journal of Media Education**, Vol. 41, Issue 21, 2013, p. 209.
4- Dianne M. Timm and Carolyn J. Duven, “Privacy and Social Networking Sites”, **New Directions for Student Services**, no. 124, 2008, p. 90.
5- David Lyon, “Surveillance, Snowden, and Big Data: Capacities, consequences, critique”, **Big Data & Society**, Vol. 1, no. 2, July-December 2014, p. 8.
6- Pew Research Center, “**Public Perceptions of Privacy and Security in the Post-Snowden Era**”, November (2014), p. 2, accessible at:http://goo.gl/wb1k4N/ (Last accessed November 2014)
7- H. Brian Holland, “Privacy Paradox 2.0”, **Widener Law Journal**, no. 19, 2010, p. 893.
8- Young and Quan-Haase, “Privacy Protection Strategies on Facebook”, **Information, Communication & Society**, Vol. 16, no. 4, 2013, p. 481
9- Pew Research Center, “**Public Perceptions of Privacy and Security in the Post-Snowden Era**”, November (2014), p. 2, accessible at: http://goo.gl/WK5iA6 / (Last accessed November 2014)
10- Young and Quan-Haase, **op.cit**., p. 482.
11- Mahsoom Thottathil, “Social Media in the MENA region [Infographic]”, **Arabian Gazette**, February 3, 2014, accessible at: http://goo.gl/Yw7UYu
12- Timothy C. Mack, “Privacy and the Surveillance Explosion”, **The Futurist**, 48:1 (2014), p. 44, accessed November 2014, www.wfs.org/futurist/january-february-2014-vol-48-no-1/privacy-and-surveillance-explosion
13- Mack, “Privacy and the Surveillance Explosion”, The Futurist, vol. 48, no. 1, 2014, p. 46
14- Lee Humphreys, “Who’s Watching Whom? A Study of Interactive Technology and Surveillance”, **Journal of Communication,** no. 61, 2011, p.576.
15- Ronald J. Deibert, **Black Code: Inside the Battle for Cyberspace,** (Toronto: McClelland & Stewart, 2013), p. 202.
16- Samuel Gibbs, “Facebook, Google and Apple lobby for curb to NSA surveillance”, **The Guardian**, November 17, 2014, accessible at: www.theguardian.com/technology/2014/nov/17/facebook-google-apple-lobby-senate-nsa-surveillance
17- Spencer Ackerman and Dominic Rushe, “Microsoft, Facebook, Google and Yahoo release US surveillance requests”**, The Guardian**, February 13, 2014, accessible at: http://goo.gl/rh4ntd
18- David Lowe, “Surveillance and International Terrorism Intelligence Exchange: Balancing the Interests of National Security and Individual Liberty”, **Terrorism and Political Violence**, August 2014, (p. 4), accessible at: http://www-tandfonline-com.nduezproxy.idm.oclc.org/doi/full/10.1080/09546553.2014.918880#.VHLFrBaUcTU (Last accessed November 2014).
19- David Lowe, **op.cit**., p. 16
20- David Lowe, **op.cit**., p. 17
21- Kamlesh Bajaj, “Cyberspace: Post-Snowden”, **Strategic Analysis**, Vol. 38, Issue 4, 2014, p. 584.
22- The Associated Press, “Senate blocks NSA phone records measure”, **Al Jazeera America,** November 19, 2014, accessible http://goo.gl/rh4ntd