الخصوصية المعلوماتية واهميتها ومخاطر التقنيات الحديثة عليها

الاستاذ المساعد الدكتور منى تركي الموسوي

المدرس جان سيريل فضل الله

مركز بحوث السوق وحماية المستهلك

جامعة بغداد

الخلاصة

أن حاجة الانسان بأن يخلو إلى نفسه وأن يشعر بالهدوء والسكينة بعيدا عن أعين الناس او مراقبة الفضوليين أو الإحتفاظ بافكاره أو علاقاته الحميمة أو ارتباطاته وأفراد أسرته وراء ستار السرية ، حاجة قديمة قدم وجود الانسان نفسه.

لذا تحرص المجتمعات خاصة الديمقراطية منها على كفالة الخصوصية، وتعتبره حقا مستقلا قائما بذاته، ولا تكتفي بسن القوانين لحمايته بل تسعي إلى ترسيخه في الأذهان، وذلك بغرس القيم النبيلة التي تلعب دورا كبيرا وفعالا في منع المتطفلين من التدخل في خصوصيات الآخرين وكشف أسرارهم. ولقد حظي هذا الحق باهتمام كبير سواء من جانب الهيئات والمنظمات الدولية أو من جانب الدساتير والنظم القانونية،

ولقد تضاعف الاهتمام بهذا الحق نظرا لما يتعرض له من مخاطر تحيط به وتهدده أبرزها التقدم التكنولوجي والإعلامي و المعلوماتى الملحوظ والذي كان له دور كبير في اقتحام حصون هذا الحق واختراق حواجزه وتسلق أسواره، الأمر الذي يقتضي تدخل المشرع لحمايته بالأسلوب الذي يتفق وطبيعة هذه الأخطار

وفي العصر الحديث ظهرت الحاجة الماسة لمعرفة الكثير من المعلومات وأصبحت المعلومات عصب الحياة الاقتصادية والسياسية والاجتماعية والعلمية. واصبح استخدام الحاسب الآلي من سمات وضرورات حسن التنظيم الاداري سواء على مستوى روابط القانون العام أو على روابط القانون الخاص. ولهذا وصف هذا العصر وبحق عصر الحاسوب.

وإذا كان موضوع البحث هو حماية الخصوصية المعلوماتية. فإنه يجدر بنا أولا بيان تعريف المقصود بهذا المصطلح وكيف أثرت فيه التكنولوجيا الحديثة.

أهمية البحث:

أن لبناء اي مجتمع رقمي يتطلب وجود نوعا من التفاعل الآمن والفوري بين خدمات الكترونية عالية المستوى، والفاعلية تقدم من قبل مؤسسات حكومية أو خاصة وبين أفراد من المجتمع يستفيدوا من تلك الخدمات . وهذا لن يتاتى إلا لو أحس الأفراد بالآمن والثقة، ومن هنا تأتي أهمية البحث في محاولة متواضعة لتسليط الضوء على الخصوصية المعلوماتية وأهميتها ومخاطر التقنيات الحديثة عليها وكيفية الحماية.

أهداف البحث:

تعد مسألة النمو المضطرد للإنترنت، من المسائل التي تشمل عمومَ الرقعة الجغرافية الكونية، وقد تحوَّلت هذه الشبكةُ المعلوماتية من أداة أكاديمية، إلى بنية عولمية راسخة لا يمكن الاستغناء عنها، فتوجَّه كثير من اهتمامات العاملين في مجتمع المعلوماتية، إلى بيان القدرات الغاشمة التي تمتلكها هذه الشبكة في توفير قدرات إضافية للإنسان المعاصر، وبرغم أننا لا ننكر الدور الفاعل لشبكة الإنترنت، وتقنيات المعلوماتية في مجتمعنا المعاصر، بَين أننا في نفس الوقت نجد أنها قد باشرت بحمل الكثير من التأثيرات الجانبية، التي تتصل بمسألة الأمن المعلوماتي لمجتمعاتنا، فهناك الكثير من التهديدات المعلوماتية التي ستطول البنى التحتية، وأخرى ستسهم في

تغيير الكثير من معالم الخارطة العقدية والثقافية للمجتمع، من أجل هذا يسعى هذا البحثُ إلى بيان أهم هذه التأثيرات، ومعالمها، وحدودها، والذي يتطلب منا المزيد من الجهد؛ لتلافي هذه التأثيرات في المستقبل القريب، فضلا عن استجلاء طبيعة التهديدات التي تفرضها تقنيات الاتصال الحديثة، وتطبيقاتها على منظومة الأمن المعلوماتي، وسبل احتوائها، والرد عليها من خلال معالجة آثارها بصحوة غامرة، تستوعب جميع مفردات حياة الفرد المعاصر.

المحور الاول: ولادة الخصوصية

مفاهيم الخصوصية[1]:

يمكن تقسيم الخصوصية إلى عدة مفاهيم ترتبط معا في الوقت ذاته وهي:

1. خصوصية المعلومات والتي تتضمن القواعد التي تحكم جميع إدارات البيانات الخاصة كمعلومات بطاقات الهوية والمعلومات المالية.
2. الخصوصية الجسدية أو المادية والتي تتعلق بالحماية الجسدية للأفراد ضد أية إجراءات ماسة بالنواحي المادية كفحص المخدرات.
3. خصوصية الاتصالات والتي تغطي سرية وخصوصية المراسلات الهاتفية والبريد الإلكتروني وغيرها من الاتصالات.
4. الخصوصية الإقليمية والتي تتعلق بالقواعد المنظمة للدخول إلى المنازل وبيئة العمل أو الأماكن العامة والتي تتضمن التفتيش والرقابة الإلكترونية.

إذن الخصوصية، وبصفة عامة، هي مقياس غير موضوعي، أي يختلف تعريفها وحدودها من بيئة إلى أخرى. ولكن الصفة المشتركة في جميع هذه التعريفات هي منظور أن الخصوصية إحدى حقوق الإنسان في حياته، ولكنها تعتمد بشكل أساسي على البيئة والسياق. اما من وجهة نظر روجر كلارك، الاستشاري والخبير في خصوصية البيانات والأعمال الالكترونية، قام بتعريف الخصوصية بأنها "قدرة الأشخاص على المحافظة على ‘مساحتهم الشخصية في مأمن من التدخل من قِبل منشآت أو أشخاص آخرين"، وقام بتحديد مستويات (أبعاد) من الخصوصية وهي:

1- خصوصية الشخص (Privacy of the person): والمعنية بسلامة الفرد في جسده، مثل قضايا التطعيم أو نقل الدم دون الحصول على موافقة الشخص المعني، أو الإجبار على تقديم عينات من سوائل الجسد أو أنسجته.

2- خصوصية السلوك الشخصي (Privacy of personal behavior): ويتصل ذلك بكل الجوانب السلوكية، وبشكل خاص الأمور الحساسة، مثل الأنشطة السياسية والممارسات الدينية، سواءً في الحياء الخاصة أو الأماكن العامة، وقد يشار إليه "بوسائل الخصوصية".

3 – خصوصية الاتصالات الشخصية (communications Privacy of personal): وهي مطالبة الأشخاص بالقدرة على الاتصال فيما بينهم دون المراقبة الروتينية من قِبل أشخاص آخرين أو منظمات، وهو ما يشار إليه أحياناً "باعتراض الخصوصية" (Deception Privacy).

4– خصوصية البيانات الشخصية (Data Privacy of personal): وهي مطالبة الأشخاص بأن لا تكون البيانات الخاصة عنهم متوفرة تلقائياً لغيرهم من الأفراد أو المنظمات، حتى في حالة أن تكون البيانات مملوكة من طرف آخر، فلهم القدرة على ممارسة قدر كبير من السيطرة أو التحكم بتلك البيانات وطريقة استخدامها. وهذا ما يعرف " بخصوصية المعلومات أو خصوصية البيانات". وعرّفها روجر "بأنها رغبة الشخص بالتحكم ،أو على الأقل التأثير بشكل كبير في كيفية التعامل مع بياناته الشخصية"[(2)].

ولادة وتطور مفهوم خصوصية المعلومات

هناك نوع من المعلومات يطلق عليها خاصة كونها تتعلق بالشخص ذاته وتنتمي إلى كيانه كإنسان مثل الإسم والعنوان ورقم الهاتف وغيرها من المعلومات ، فهي معلومات تأخذ شكل بيانات تلزم الإلتصاق بكل شخص طبيعي معرف أو قابل للتعريف.

وهذه النوعية من المعلومات أصبحت في وقتنا الحاضر على درجة كبيرة من الأهمية في ظل فلسفة المعلوماتية المعاصرة، سيما وأن فكرة العالم الرقمي، لا يمكن لها السير في التطور ومواكبة اهتمامات الإنسان سوى باستخدام المعلومات. من هنا ظهر ما يعرف بالخصوصية المعلوماتية.

ويعتبر مبدأ الخصوصية المعلوماتية الذي يقصد به حق الشخص في أن يتحكم بالمعلومات التي تخصه من المبادئ القديمة.

وعليه يمكننا القول ان خصوصية المعلومات هي حماية البيانات ، فهناك ترادف بوجه عام قائم ما بين اصطلاح خصوصية المعلومات وحماية البيانات، وليس بين الخصوصية وبين حماية البيانات، اما شيوع استخدام اصطلاح الخصوصية مستقلا ومنفردا دون الحاقه بالبيانات في البيئة الإلكترونية للدلالة على حماية البيانات واستخدامه، فهو امر يرجع الى ان تعبير الخصوصية شاع بوقعه هذا في ظل تزايد مخاطر التقنية الى مدى ارتبط بها في الاستخدام وكأنه ينحصر في نطاقها وبيئتها ، وهو طبعا ليس بكذلك، لكن ربما لان اشد ما يمكن ان يمثل تغولا على هذا الحق وانتهاكا له، هو الوسائل التقنية ومخاطر المعالجة الآلية للبيانات، كما ان استخدام اصطلاح الخصوصية في بيئة مواقع الإنترنت ومسائل عقود التقنية او خدمات التقنية عموما يشير الى حماية الخصوصية المعلوماتية او حماية البيانات.

فالخصوصية هي حق أساسي لا يموت، ولهذا فإنّهم يعتقدون أنّ القوانين ما زالت قادرة على حماية الأفراد من «الانتهاكات الالكترونية» للخصوصية، وإن كانوا يقرّون بالصعوبات التي تحول دون حماية هذا الحق بشكل مطلق، وذلك بالنظر إلى الوتيرة السريعة لتطوّر «ثورة المعلوماتية»، فضلاً عن الطابعين الكوني واللامركزي لشبكة الانترنت، مما يجعل التعامل مع ظاهرة انتهاك الخصوصية أمراً بالغ التعقيد،

ولعلّ هذه الانتهاكات قد تصل حد التسلل إلى ملفاتنا الشخصية، وربما مراقبتنا عبر الكاميرات المثبتة في أجهزة الكومبيوتر الخاصة بنا من دون أن نشعر بذلك، وهو أمر «وإن كانت القدرة عليه متفاوتة بالنظر إلى نظم الحماية والتشفير التي يعكف المبرمجون على تطويرها بشكل مستمر، إلا أنّه يبقى ممكناً، أقله من الناحية النظرية».

ان فكرة الخصوصية وارتباطها بتقنية المعلومات هي أول مسائل قانون الكمبيوتر عموما من الوجهة التاريخية، وهي اول مناطق التساؤل عن اثر التقنية على النظام القانوني ومسائله، وقد انطلقت في الستينات وفي اجواء التطور التكنولوجي الواسع وأجواء الاستخدامات المتزايدة للحوسبة وانشاء بنوك المعلومات وعمليات المعالجة الالية للبيانات، وفي سياق حماية الافراد من مخاطر التقنية التي تتهدد حياتهم الخاصة، فتمس على نحو مباشر خصوصياتهم واسرارهم، ولهذا ارتبطت ولادة مفهوم خصوصية المعلومات بالخشية من مخاطر التقنية ذاتها.

ان الدراسات القانونية الأكاديمية التي عنيت بالخصوصية وبحقوق الانسان في ضوء التطورات التقنية محدودة بشكل عام، ويمكن القول ان نهاية الستينات والسبعينات شهدت انطلاق مثل هذه الدراسات، وان هذه الفترة تحديدا هي التي أثير فيها لاول مرة وبشكل متزايد مفهوم خصوصية المعلومات كمفهوم مستقل عن بقية مفاهيم الخصوصية وتحديدا التدخل المادي ومسائل الرقابة، ويعزى الفضل في توجيه الانتباه لمفهوم خصوصية المعلومات في هذه الفترة الى مؤلفين أمريكيين هامين في هذا الحقل، الأول كتاب الخصوصية والحرية Privacy and Freedom لمؤلفه ويستن – Alan Westin عام 1967[3]، والثاني كتاب الاعتداء على الخصوصية The Assault on Privacy لمؤلفه ميلر Miller[4]، وكلاهما قدما مفهوما وتعريفا لخصوصية المعلومات.

فوفقا لـ (ويستن)، فان خصوصية المعلومات تعني " حق الافراد في تحديد متى وكيف والى أي مدى تصل المعلومات عنهم للاخرين" (the claim of individuals 'to determine for themselves when, how and to what extent information about them is communicated to others)، في حين جاء تعريف ميلر اكثر عمقا – مع ان ويستن يعتبر منظر الحق في خصوصية المعلومات – اذ عرف خصوصية المعلومات بانها "قدرة الافراد على التحكم بدورة المعلومات التي تتعلق بهم" ('the individual's ability to control the circulation of information relating to him').

ومن خلاصة هذه الدراسات الأكاديمية في الفترة المشار إليها، يمكن القول أن الخصوصية من حيث مفهومها جرى التعامل معها كحق لمنع إساءة استخدام الحكومة للبيانات التي يصار لمعالجتها آليا او الكترونيا أو تقييد استخدامها وفق القانون فقط.

وقد كان للتطورات التقنية، وتحديدا إنشاء بنوك المعلومات وإجراء عمليات المعالجة والتحليل بواسطة الكمبيوترات، الأثر في خلق مفهوم خصوصية المعلومات بالمحتوى المشار اليه، وقد كان الفقهاء المتقدم الاشارة اليهم (وسيترن وميلر ورولي) من اوائل من ساهموا في اثارة مسائل نظام خصوصية المعلومات وتوضيح ملامحه.

وفي ذات الفترة ، قامت الدول الغربية بسن تشريعات حماية البيانات انطلاقا من مطلع التسعينات وترافق ذلك مع دراسات مقارنة بين القوانين الوطنية، وفي هذا الصدد يبرز مثلا جهد الكاتب بوركرت Burkert [5] وناغتر Nugter [6]خلال الثمانينات وبداية التسعينات.

وقد شهد عام 1994 اعداد دراسات واسعة بشان المسائل المتصلة بالخصوصية وحقوق الانسان عالميا في ضوء التطورات التقنية الحديثة، منها مثلا الدراسة التي اعدها البروفسور ميشيل Michael بعنوان (الخصوصية

وحقوق الانسان – Privacy and Human Rights)[7]، تحت اشراف اليونسكو، حيث قام المؤلف بتقييم المحتوى الاجتماعي والسياسي والثقافي المتضمن في تشريعات الخصوصية وحماية البيانات عالميا. والمفيد في مؤلف ميشيل انه استعرض الصعوبات والتباينات الثقافية في استخدام اصطلاح الخصوصية واختلاف المفهوم القانوني ايضا للخصوصية بين النظم القانونية المختلفة وفي نطاق المفهوم القانوني للخصوصية اوضح هذا المؤلف ثلاث مواقف (موقف مؤتمر دول الشمال الاوروبي، موقف نظام القانوني المدني – اللاتيني ، وموقف نظام القانون العام – الانجلوامريكي) فعرض في نطاق المفهوم الاول، موقف لقاء الخبراء القانونيين في ستوكهولم عام 1967 الذي نتج عنه اعلان غير ملزم حول معنى الحق في الخصوصية تضمن المبادئ التي قام عليها فيما بعد اول تشريع شمولي للحماية البيانات وهو القانون السويدي لعام 1973 كما سنرى. وقد اعتبر هذا الاعلان خصوصية المعلومات مزيج من مكنات او حقوق الافراد من خلال التوازن بين الحق في الوصول للمعلومات والتنظيمات الادارية لملفات الكمبيوتر a combination of legal remedy available to the individual through rights of access and the administrative regulation of computerized records.

لماذا الانترنت مختلفة عن غيرها من الوسائل في علاقتها بالخصوصية :-

ان وضع نظام لحماية الخصوصية في بيئة الانترنت عليه ان يراعي طبيعة التهديدات الخاصة التي تتعرض لها الخصوصية في نطاق استخدام عمليات الانترنت، فالإنترنت تخلق سلسلة من التحديات الجديدة في مواجهة خطط حماية المستهلك والطفولة وحماية الخصوصية، وتتمثل هذه التحديات بما ياتي[8]:-

١ +الإنترنت تزيد كمية البيانات المجمعة والمعالجة والمنشاة .

ان الإنترنت شهدت نماء التوجه نحو جمع البيانات المتوفرة في العالم الحقيقي باعتبارها تصبح اكثر سهولة في بيئة الانترنت من حيث قدرة الوصول اليها، واكثر ملاءمة للتبويب بسبب تقنيات الحوسبة، وتصبح اسهل للتبادل في ضوء وسائل تبادل المعلومات بكل اشكالها التي اتاحتها الانترنت وبرمجيات التصفح والتبادل والنقل.

فالبيئة التي تمر عبرها رحلة البيانات المتبادلة تغيرت بسبب الانترنت، وترك الأفراد خلفهم الوسائل التقليدية في الوصول للمعلومات واصبح اعتمادهم اكثر فاكثر على الإنترنت، لان الانترنت مصدر غني بالمعلومات حول كل شيء، وفي نطاق مسائل الخصوصية تحديدا فان المعلومات عن الافراد وعاداتهم وهواياتهم ومسلكياتهم وآرائهم واتجاهاتهم في التسوق أصبحت متوفرة في ظل الانترنت.

ان البيانات المنقولة والمتبادلة والتي يطلق عليها تعبيرات عديدة كنهر المعلومات المتدفق، قد تشمل عنوان بروتوكول الانترنت لحواسيب الافراد، المتصفحات المستخدمة، نوع الحاسوب المستخدم، وآخر ما قام به المستخدم في زيارته الاخيرة للموقع وربما المواقع الاخرى التي زارها ، فهذه المعلومات التي قد تكون كافية للتعريف عن الشخص، يتم اصطيادها وجمعها في نقاط عديدة في الرحلة عبر الشبكات، ويمكن ان تتوفر لاعادة استخدامها او افشائها او تناقلها بين قطاعات معنية بجمعها، وبعض هذه المعلومات قد تكون مهمة وضرورية لعمليات الشبكة والوصول لمواقع الانترنت، كرقم التلفون وعنوان بروتوكول الانترنت الخاص، وبدونهما فالشبكة غير قادرة على العمل، ولكن هناك اجزاء من المعلومات قد لا تكون ضرورية لهذه العمليات وقد يكون جمعها لاغراض غير

عمليات الشبكة، ومع المعلومات التي تجمع في مراحل شراء المنتجات او لمجرد التسجيل او الاشتراك بخدمات الموقع، فان جمع هذه المعلومات قد يشكل بيانا بانشطة الفرد، وفي مرحلة من المراحل تصبح هذه البيانات عند جمع شتاتها وتحليلها مادة تكشف تفاصيل كثيرة قد لا يرغب الشخص بكشفها، وبنفس الوقت تصبح هذه البيانات مادة غنية ومحلا للبيع من جهة لاخرى لغايات الاعمال والانشطة.

٢ – الإنترنت أتاحت عولمة المعلومات والاتصالات .

في بيئة الانترنت، تتدفق المعلومات والاتصالات عبر الحدود دون اي اعتبار للجغرافيا والسيادة ، والافراد يعطون معلوماتهم لجهات داخلية وخارجية وربما جهات ليس لها مكان معروف، وهو ما يثير مخاطر اساءة استخدام هذه البيانات خاصة في دول لا تتوفر فيها مستويات الحماية القانونية للبيانات الشخصية. وقد لا تخدم القوانين الوطنية كثيرا في هذا الفرض، كما ان تضمينها نصوصا بشان السيطرة على نقل البيانات قد لا يكون فاعلا في ظل غياب التنسيق وضمان ان يكون نقل البيانات محكوما باتفاقات تكفل حمايتها او تضمن توفر حماية مماثلة في الدولة المنقول لها البيانات، وتعدو المخاطر اوسع مع نشوء ملاجئ آمنة لا تقيد عمليات المعالجة باي قيد ولا تتوفر عندها قيود منعية على جمع ومعالجة البيانات، وهي ملاجئ تهرب اليها مؤسسات الاعمال في بيئة الانترنت للافلات من القيود القانونية، تماما كما في حالات البحث عن ملاجئ لا تفرض فيها الضرائب او تتيح تبادل الاموال دون رقابة، وهذه تمثل تحديا عالميا وليس مجرد تحد وطني، ولعلها الاساس الذي يدفع نحو ابرام اتفاقيات ثنائية وعالمية في حقل حماية البيانات الشخصية عبر الحدود وهو نفس الاساس الذي اوجب ايجاد الادوات العقدية التي تفرض على الجهة متلقية البيانات او الوسيطة في تلقيها لارسالها لطرف ثالث التزامات قانونية معينة تدور في مجموعها حول هدف حماية الخصوصية ومنع اساءة استخدام بيانات الافراد الخاصة الى جانب غرضها في منع الانشطة الاحتيالية والمساس بالمستهلك في بيئة الانترنت.

٣ – التحدي الناشئ عن فقدان المركزية وآليات السيطرة والتحكم .

ان اقرار قانون وطني او تطوير استراتيجية وطنية ملائمة لحماية احد حقوق الانسان ، قد يكون فاعلا ويرجع ذلك لعنصر السيطرة والسيادة وتوفر الجهة القادرة على الرقابة ومنع الاعتداء او استمراره، والتي تتيح ايضا التعويض وملاحقة المخالفين ، لكن كيف يكون الوضع في ظل الانترنت التي يملكها كل شخص وغير مملوكة لاحد، والتي لا تتوفر فيها سلطة مركزية ولا جهة سيادة توفر الحماية او تتيح الفرصة والمكنة للحماية القانونية عند حدوث الاعتداء.

وبالرغم من ان الصراع يحتدم على السيطرة على الانترنت، من خلال السعي للسيطرة على أسماء النطاقات وعناوين المواقع، والتنافس للسيطرة على سوق استضافة المواقع عبر الخوادم التقنية والتوجه احيانا للتحكم بالمعلومات وطرق تبادلها عبر التحكم بالحلول التقنية واحتكارها لتكون وسيلة التحكم بمصائر المستخدمين واداة السيطرة الفعلية، وبالرغم من كل ذلك، ومع ما يرافقه من نشاط مضاد لجهة منع الاحتكار المعلوماتي وتباين المصالح بين أمريكا وأوروبا وشرق اسيا في هذا الشان، فان الانترنت تتصف باللامركزية وغياب السلطة التحكمية،

وليس الدعوات انشاء حكومة الانترنت او بوليس الانترنت او معايير الاستخدام الموحد او سياسات التنظيم الذاتي للالتزامات الا وسائل افتراضية شانها شان البيئة التي نشأت فيها، ومن هنا يكون لبعض مسائل التعاون الدولي أهمية بالغة، ابرزها الاتفاق في حقل الاختصاص القضائي والقانون الواجب التطبيق في بيئة منازعات الانترنت.

ومع وجود توجهات للتعاون والتنظيم الدولي، وجهود مميزة لدى منظمة التعاون الاقتصادي والتنمية، والاتحاد الاوروبي، وجهات تقنية وهيئات وقطاعات عاملة في بيئة الانترنت، فان كافة هذه الجهود حتى الان لم تقدم حلولا للمشكلات لعدم وجود تنظيم مقبول يحكم الانترنت في كل مسائلها، ولعل طبيعة الانترنت واتجاهات تطور طريق المعلومات السريع يعطي انطباعا ان الانترنت ستبقى خارج أمنيات الحكومات في ايجاد تنظيم قانوني يحكمها او يسيطر على شؤونها.

ان البيانات تنتقل عبر الانترنت من دولة لدولة ومن منظمة لمنظمة ومن جهة عمل الى اخرى، من فرد الى مؤسسة، دون قيود وبكل اللغات وتسافر المعلومة عبر الشبكات المحلية فالمناطقية فالدولية، وتوجه من نقطة لاخرى في الفضاء، وفي رحلتها هذه تحط وتزور العديد من مناطق الاختصاص القضائي ومناطق السيادة، ومناطق قد لا تكون بينها تعاون او حتى روابط، ففي مثل هذه البيئة ثمة حاجة لجهد استثنائي على النطاق الدولي، أهم ما يتعين ان يتصف به الخروج من الاطر والمفاهيم التقليدية للسيطرة، فلم تعد ارادة القوي هي حجر الزاوية، فربما يكون لفرد ما القدرة في هكذا بيئة ان يتحدى اعظم القوى، لهذا فان ما نسميه ديمقراطية الانترنت، وعدالة التعامل مع المعرفة، وعدم التمييز وانتهاء عهد الاحتكار والسيطرة، هي الاسس التي يتعين ان يتم التفكير فيها في كل نشاط يهدف الى تنظيم ضروري لمسائل الانترنت، والاهم ان يكون تنظيما يراعي هذه السمات التقنية وهذه الخصائص وميزات التفاعلية اللامتناهية.

المحور الثاني: المخاطر المهددة للخصوصية

التقنيات الحديثة وأثرها على الخصوصية المعلوماتية

تتزايد مخاطر التقنيات الحديثة على حماية الخصوصية ، كتقنيات رقابة (كاميرات) الفيديو، وبطاقات الهوية والتعريف الإلكترونية، وقواعد البيانات الشخصية، ووسائل اعتراض ورقابة البريد والاتصالات، ورقابة بيئة العمل وغيرها[9] .

وبفعل الكفاءة العالية للوسائل التقنية والإمكانات غير المحدودة في مجال تحليل واسترجاع المعلومات، اتجهت جميع دول العالم بمختلف هيئاتها ومؤسساتها الى إنشاء قواعد البيانات لتنظيم عملها، واتسع على نحو كبير استخدام الحواسيب لجمع وتخزين ومعالجة البيانات الشخصية لأغراض متعددة فيما يعرف ببنوك ومراكز المعلومات الوطنية، ومع تلمس المجتمعات لإيجابيات استخدام الحواسيب في هذا المضمار ظهر بشكل متسارع أيضا، الشعور بمخاطر تقنية المعلومات وتهديدها للخصوصية. هذا الشعور نما وتطور بفعل الحالات الواقعية للاستخدام غير المشروع للبيانات الشخصية واتساع دائرة الاعتداء على حق الأفراد في الحياة الخاصة مما حرك الجهود الدولية والإقليمية والوطنية، لإيجاد مبادئ وقواعد من شأن مراعاتها لحماية الحق في الحياة الخاصة، وبالضرورة إيجاد

التوازن بين حاجات المجتمع لجمع وتخزين ومعالجة البيانات الشخصية، وكفالة حماية هذه البيانات من مخاطر الاستخدام غير المشروع لتقنيات معالجتها.

وإذا كانت الجهود الدولية والاتجاه نحو الحماية التشريعية للحياة الخاصة عموما، وحمايتها من مخاطر استخدام الحواسيب وبنوك المعلومات على نحو خاص، تمثل المسلك الصائب في مواجهة الأثر السلبي للتقنية على الحياة الخاصة، فان هذا المسلك قد رافقه اتجاه متشائم لاستخدام التقنية في معالجة البيانات الشخصية. فالتوسع الهائل لاستخدام الحواسيب قد أثار المخاوف من إمكانات انتهاك الحياة الخاصة، ومكمن إثارة هذه المخاوف، أن المعلومات المتعلقة بجميع جوانب حياة الفرد الشخصية، كالوضع الصحي والأنشطة الاجتماعية والمالية والسلوك والآراء السياسية وغيرها، يمكن جمعها وخزنها لفترة غير محددة، كما يمكن الرجوع إليها جميعا بمنتهى السرعة والسهولة. ومع الزيادة في تدفق المعلومات التي تحدثها الحواسيب، تضعف قدرة الفرد على التحكم في تدفق المعلومات عنه[10].

يقول" Robert M.Bowie :- أن التقنوقراطية، وهي تملك الكمبيوترات قد تصبح على درجة بالغة من القوة بحيث تحبس الحياة الخاصة داخل حدود ضيقة، وتكيف حياة الفرد وأسرته بهذه الأجهزة في اللحظة التي تكون لها في ذلك مصلحة اقتصادية أو اجتماعية، وبذلك يصبح الإنسان معاملا كالأرقام بكمبيوتر مسلوب الإرادة في اتخاذ قراراته بوعي واستغلال، ومفرغا أخيرا من شخصيته "، أن ما يهدد الجنس البشري ليس حربا نووية ، بل جهاز كمبيوتر[11].

أن هذه النظرة – كما يظهر لنا، نظرة متشائمة من شيوع استخدام الحواسيب واثرها على تهديد الخصوصية، وهي وان كانت نظرة تبدو مبالغا فيها، الا أنها تعكس حجم التخوف من الاستخدام غير المشروع للتقنية، وتحديدا الحواسيب، في كل ما من شأنه تهديد الحق في الحياة الخاصة، ويمكننا فيما يلي إجمال المعالم الرئيسة لمخاطر الحواسيب وبنوك المعلومات على الحق في الحياة الخاصة بما ياتي[12]-:

أولا: "أن الكثير من المؤسسات الكبرى والشركات الحكومية الخاصة، تجمع عن الأفراد بيانات عديدة ومفصلة تتعلق بالوضع المادي أو الصحي أو التعليمي أو العائلي أو العادات الاجتماعية أو العمل ..الخ، وتستخدم الحاسبات وشبكات الاتصال في خزنها ومعالجتها وتحليلها والربط بينها واسترجاعها ومقارنتها ونقلها، وهو ما يجعل فرص الوصول الى هذه البيانات على نحو غير مأذون به أو بطريق التحايل اكثر من ذي قبل، ويفتح مجالا أوسع لإساءة استخدامها أو توجيهها توجيها منحرفا أو خاطئا أو مراقبة الأفراد وتعرية خصوصياتهم أو الحكم عليهم حكما خفيا من واقع سجلات البيانات الشخصية المخزنة [12]. على سبيل المثال، فأن حكومة الولايات المتحدة وفق دراسات 1990 جمعت (4) بليون سجل مختلف حول الأمريكيين، بمعدل (17) بندا لكل رجل وامرأة وطفل، ومصلحة الضريبة (IRS) في الولايات المتحدة تمتلك سجلات الضرائب لحوالي (100) مليون أمريكي على حواسيبها.

ثانيا : أن شيوع (النقل الرقمي) للبيانات خلق مشكلة أمنية وطنية، إذ سهل استراق السمع والتجسس الإلكتروني. ففي مجال نقل البيانات، تتبدى المخاطر المهددة للخصوصية في عدم قدرة شبكات الاتصال على توفير الأمان المطلق أو الكامل لسرية ما ينقل عبرها من بيانات، وامكانية استخدام الشبكات في الحصول بصورة غير مشروعة

عن بعد على المعلومات، ولم تحل وسائل الأمان التقنية من الحماية من هذه المخاطر فعلى سبيل المثال، وجه الرئيس الأمريكي ريغان عام 1984 الى شبكة (NEA) الدعوة للبحث عن طرق تنتج شبكات هاتفية آمنة بشكل اكبر للاتصالات الخاصة بالمعلومات الحكومية الحساسة، الا أن تكاليف تركيب هواتف آمنة وبمساعدة نبائط الخلط تعتبر عالية، وقد كشفت شركة (BT بريتيش تيليكوم) في المملكة المتحدة النقاب في عام 1986 عن نبيطة على شكل شريحة تقوم بالتشفير وتعمل على خلط المعلومات بما يتيح التمويه قبل أن يتم إرسالها على خطوط المواصلات، لكن الواقع العملي كشف عن استخدام وسائل تقنية تبطل مفعول مثل هذه النبائط الإلكترونية وفي الاعوام من 1993 وحتى 2000 نشط البيت الابيض الامريكي والهيئات المتخصصة التي انشأها لهذا الغرض في توجيه جهات التقنية الى العمل الجاد على خلق تقنيات أمان كافية للحفاظ على السرية الخصوصية، وبالرغم من التقدم الكبير على هذا الصعيد الا ان احدث تقارير الخصوصية تشير الى انه لمتزل حياة الافراد واسرارهم في بيئة النقل الرقمي معرضة للاعتداء في ظل عدم تكامل حلقات الحماية (التنظيمية والتقنية والقانونية).

ثالثا : أن اكثر معالم خطر بنوك المعلومات على الحياة الخاصة، ما يمكن أن تحويه من بيانات غير دقيقة أو معلومات غير كاملة لم يجر تعديلها بما يكفل إكمالها وتصويبها[1]. فعلى سبيل المثال، كلف مكتب تقييم التقنية في الولايات المتحدة (OTA) في عام 1981 الدكتور (لوردن)، وهو عالم في مجال الجريمة، بإجراء دراسة حول قيمة بيانات التاريخ الإجرامي التي تحويها ملفات (FBI– وكالة الشرطة الفدرالية) وملفات وكالة شرطة ولاية نيويورك، وقد وجد أن النسبة عالية من البيانات كانت غير كاملة وغير دقيقة ومبهمة، ويتضمن العديد منها اعتقالات وتقصيات لم تؤد الى إدانة، أو أنها متعلقة بجنح بسيطة تمت في الماضي القديم، واظهرت دراسات أخرى أن أصحاب العمل لم يوظفوا في الغالب مثل هؤلاء الأشخاص لسجلاتهم الإجرامية غير الدقيقة.

رابعا : "أن المعلومات الشخصية التي كانت فيما قبل منعزلة متفرقة، والتوصل إليها صعب متعذر، تصبح في بنوك المعلومات مجمعة متوافرة متكاملة سهلة المنال، متاح اكثر من ذي قبل استخدامها في أغراض الرقابة على الأفراد، وهكذا تبدو صائبة مقولة ارثر ميللر:– أن الحاسب بشراهته التي لا تشبع للمعلومات، والسمعة التي ذاعت حول عدم وقوعه في الخطا وذاكرته التي لا يمكن لما يختزن فيها أن ينسى أو ينمحي، قد تصبح المركز العصبي (Centre Nerveax) لنظام رقابي يحول المجتمع الى عالم شفاف ترقد فيه عارية بيوتنا ومعاملاتنا المالية، واجتماعاتنا وحالتنا العقلية والجسمانية لأي مشاهد عابر[12].

خامسا :– ان تكامل عناصر الحوسبة مع الاتصالات والوسائط المتعددة اتاح وسائل رقابة متطورة سمعية ومرئية ومقروءة، اضافة الى برمجيات التتبع وجمع المعلومات آليا، كما اتاحت الانترنت – واسطة هذه العناصر جميعا – القدرة العالية لا على جمع المعلومات فقط، بل معالجتها عبر تقنيات الذكاء الصناعي التي تتمتع بها الخوادم (انظمة الكمبيوتر المستضيفة وانظمة مزودي الخدمات) والتي تتوفر ايضا لدى محركات البحث وبرمجيات تحليل الاستخدام والتصرفات على الشبكة، بحيث لا يستغرب معها ان الشخص عندما يتصل باحد مواقع المعلومات البحثية في هذه الايام يجد امامه المواقع التي كان يفكر في دخولها والتوصل بها، كما لا يستغرب مستخدم الانترنت ان ترده رسائل بريد الكتروني تسويقية من جهات لم يتصل بها تغطي ميوله ورغباته[13].

ان بدء مشكلات الكمبيوتر في الستينات ترافق مع الحديث – في العديد من الدول الغربية – عن مخاطر جمع وتخزين وتبادل ونقل البيانات الشخصية ومخاطر تكنولوجيا المعلومات في ميدان المساس بالخصوصية والحريات العامة، وانتشر الحديث عن الخطر الكبير التي يتهدد الحرية الشخصية بسبب المقدرة المتقدمة لنظم المعالجة الالكترونية على كشف والوصول الى المعلومات المتعلقة بالأفراد واستغلالها في غير الاغراض التي تجمع من اجلها. وخلال الثمانينات تغير الواقع التكنولوجي فيما يتعلق بالجهات التي تملك وتسيطر على نظم الكمبيوتر وكان ذلك بسبب اطلاق الحواسيب الشخصية وانتشارها، واصبح من الواضح ان حماية الخصوصية يتعين ان تمتد الى الكمبيوترات الخاصة وان يتم احداث توازن ما بين الحق في الخصوصية او الحق في الحياة الخاصة وبين الحق في الوصول الى المعلومات، هذا التغير في الواقع التكنولوجي عكس نفسه على حقل الحماية القانونية في الخصوصية بأبعادها التنظيمية والمدنية والجزائية وبدأت تكثر الاحاديث بشأن دعاوى الاستخدام غير المشروع للمعلومات وللوثائق الشخصية، وظهرت احداث شهيرة في حقل الاعتداء على البيانات الخاصة من بينها – على سبيل المثال – الحادثة التي حصلت في جنوب افريقيا حيث امكن للمعتدين الوصول الى الاشرطة التي خزنت عليها المعلومات الخاصة بمصابي امراض الايدز وفحوصاتهم، وقد تم تسريب هذه المعلومات الخاصة والسرية الى جهات عديدة. ومن الحوادث الشهيرة الاخرى حادثة حصلت عام 1989 عندما تمكن احد كبار موظفي احد البنوك السويسرية بمساعدة سلطات الضرائب الفرنسية بان سرب اليها شريطا يحتوي على أرصدة عدد من الزبائن، وقد تكرر مثل هذا الحادث في المانيا ايضا. وقد اظهرت القضايا التي حصلت ما بين عامي 96–97 في الحقل المصرفي ان الوصول الى البيانات الشخصية ارتبط في الغالب بانشطة الابتزاز التي غالبا ما تتعلق بالتحايل على الضريبة من قبل زبائن البنوك[14].

وفي عام 1986 اتهمت شركة IBM بان نظام الامن التي تنتجه المسمى RACF يستخدم للرقابة على الموظفين داخل المنشآت، وفي عام 1994 ايضا وفي المانيا اثير جدل واسع حول حق دائرة التأمينات الصحية بنقل البيانات الشخصية الى شركات خارجية، وشبيه بهذا الجدل ما يثور الان بشأن مدى احقية شركات تزويد الانترنت والتلفونات الكشف عن معلومات الزبائن لجهات اخرى.

ان هذه المخاطر اثارت وتثير مسالة الاهمية الاستثنائية للحماية القانونية – الى جانب الحماية التقنية للبيانات الشخصية، ومن العوامل الرئيسة في الدفع نحو وجوب توفير حماية تشريعية وسن قوانين في هذا الحقل، انه وقبل اختراع الكمبيوتر، فان حماية هؤلاء الاشخاص كانت تتم بواسطة النصوص الجنائية التي تحمي الاسرار التقليدية(كحماية الملفات الطبية او الاسرار المهنية بين المحامي والموكل) وعلى الرغم من ذلك فان هذه النصوص التقليدية لحماية شرف الانسان وحياته الخاصة لا تغطي الا جانبا من الحقوق الشخصية وبعيدة عن حمايته من مخاطر جمع وتخزين والوصول الى ومقارنة واختيار وسيلة نقل المعلومات في بيئة الوسائل التقنية الجديدة هذه المخاطر الجديدة التي تستهدف الخصوصية دفعت العديد من الدول لوضع تشريعات ابتداءا من السبعينات، تتضمن قواعد ادارية ومدنية وجنائية من اجل حماية الخصوصية وتوصف بانها تشريعات السرية. كما أن هذه المخاطر، وما يتفرع عنها من مخاطر أخرى – كتلك الناتجة عن معالجة البيانات في شبكات الحواسيب المربوطة ببعضها البعض والتي تتيح تبادل المعلومات بين المراكز المتباعدة و المختلفة من حيث أغراض تخزين البيانات بها – نقول، أن

هذه المخاطر كانت محل اهتمام دولي وإقليمي ووطني افرز قواعد ومبادئ تتفق وحجم هذه المخاطر، كوجوب مراعاة الدقة في جمع البيانات وكفالة صحتها وسلامتها، واتخاذ تدابير أمنية لمعالجتها وخزنها ونقلها، واقرار مبدأ حق المشاركة الفردية في تعديل وتصحيح وطلب إلغاء البيانات، ووجوب تحديد الغرض من جمعها ومدة استخدامها، واقرار مبدأ مسؤولية القائمين على وظائف بنوك المعلومات لأي تجاوز أو مخالفة للمبادئ الموضوعية والشكلية في جمع ومعالجة وتخزين ونقل البيانات الشخصية، وهذه المبادئ أكدت عليها ايضا تشريعات حماية الحياة الخاصة.

والحقيقة أن استخدام وسائل التقنية العالية في ميدان جمع ومعالجة البيانات الشخصية من قبل الدولة أو القطاع الخاص، قد عمق التناقضات الحادة التي برزت منذ القدم بين حق الأفراد في الحياة الخاصة، وموجبات اطلاع على شؤون الأفراد، وتتمثل هذه التناقضات، بمعالم أربعة رئيسة-:

أولا -: التناقض بين حق الحياة الخاصة وحق الدولة في الاطلاع على شؤون الأفراد، والذي عمقه تزايد تدخل الدولة في شؤون الأفراد ، وليس المراد بهذا التدخل الاطلاع على معلومات معينة عن الأفراد لتنظيم الحياة الاجتماعية على نحو افضل، كالاحتفاظ بسجلات الولادات والزواج والوفيات والإحصاءات وغيرها، بل استخدام الدولة للمعلومات الشخصية الخاصة بالفرد لأغراض تتناقض مع صونها واحترامها.

ثانيا -: التناقض بين حق الفرد في الاحتفاظ بسريته، ومصلحته في كشف حياته الخاصة ليتمتع بثمار هذا الكشف ورغم أن هذا التناقض للوهلة الاولى غير متحقق، باعتبار أن الاحتفاظ بالسرية حق، والكشف الطوعي عن هذه السرية حق أيضا، الا أن احتمال استغلال المعلومات المعطاة طوعا لأغراض غير التي أعطيت لأجلها يمثل انتهاكا لحرمة الفرد وسريته.

ثالثا -: التناقض بين الحياة الخاصة، والحق في جمع المعلومات لغايات البحث العلمي، أو حرية البحث العلمي.

رابعا -: التناقض بين الحق في الحياة الخاصة وبين حرية الصحافة وتبادل المعلومات (الحرية الاعلامية).

هذه التناقضات – كما اسلفنا – برزت منذ القدم بين حق الفرد في حماية حياته وبياناته الخاصة، وبين موجبات الاطلاع على شؤون الفرد، بما فيها تلك التي تقع ضمن نطاق حياته الخاصة. وإذا كانت الجهود التنظيمية، الإدارية والتشريعية، سعت الى إقامة التوازن بين هذه الحقوق المتعارضة فان استخدام التقنية في ميدان جمع ومعالجة البيانات الشخصية، قد خلق واقعا صعبا هدد هذا التوازن من جهة وعمق حدة التناقضات المشار إليها من جهة أخرى.

مخاطر الخصوصية في بيئة الإنترنت والتجارة الإلكترونية[15]

إنّ «مسألة الخصوصية بدأت تظهر مع انتشار استخدام أجهزة الحاسب الآلي في السبعينيات، حين تبيّن أن المعالجة الآلية للبيانات والمعلومات يمكن أن تنجم عنها مخاطر جدّية تطال الحياة الخاصة للأفراد، خصوصاً إذا تمت هذه المعالجة من دون علم أصحابها أو موافقتهم الصريحة،

وأن ما يزيد من هذه التحديات هو أن الانترنت «شبكة مشرّعة وغير مركزية، إذ لا وجود لسلطة وحيدة تديرها أو تتحكم بتدفق المعلومات والبيانات عبرها، فضلاً عن طبيعتها الكونية التي تشكل عنصر تعقيد إضافي ناتج عن عدم خضوع هذه الشبكة إلى قوانين أو محاكم محددة.

أنّ» الدول التي أدركت باكراً حجم هذه المسألة، بادرت منذ السبعينيات إلى إصدار تشريعات خاصة بحماية الحياة الفردية. وقد عمدت هذه الدول، لا سيما الأوروبية منها، إلى تحديث تشريعاتها تباعاً، وذلك مع تقدم التقنيات»، موضحاً أنّ من بين ما تفرضه هذه التشريعات «موجب الالتزام بالغاية المحددة مسبقاً من جمع المعلومات»، و«عدم التصرف بها من دون موافقة أصحابها»، فضلاً عن منح مجموعة من الحقوق للأفراد، من بينها «حق الوصول إلى المعلومات لتصحيحها.

أن الإنترنت اكبر آلة جمع ومعالجة ونقل للبيانات الشخصية ان تطوير الحواسيب الرقمية وتكنولوجيا الشبكات، وبشكل خاص الإنترنت اتاح نقل النشاط الاجتماعي والتجاري والسياسي والثقافي والاقتصادي من العالم المادي الى العالم الافتراضي البيئة الالكترونية، ويوماً بعد يوم تتكامل الشبكات العالمية للمعلومات مع مختلف انشطة الحياة ، وبنفس الوقت فان التطور الثقافي في توظيف التقنية رافقه توجه واسع بشأن حماية خصوصية الأفراد.

أنّ خرق الخصوصية على شبكة الانترنت يمكن أن يتم من قبل جهات ثلاث أساسية هي: مزوّد خدمة الاتصال بالانترنت(Internet Service Provider)، والمواقع التي يزورها المتصفح، بالإضافة إلى مخترقي الشبكة (Hackers)أفراداً أو أجهزة أمنية واستخباراتية.

أن باستطاعة مزوّد الخدمة أن يرصد كل ما تقوم به على الانترنت (مكان وزمان الدخول إلى الشبكة، المواقع التي تم تصفّحها، الكلمات التي جرى البحث عنها، الحوارات، الرسائل الالكترونية المتبادلة... إلخ)، وذلك من خلال رقم الانترنت الخاص بالمستخدم (Internet Protocol) ، وأدوات أخرى تعرف بالـ «Proxy»و «Packet Sniffer»، وهي برمجيات قادرة على تحليل كل حركة تجري على الشبكة الالكترونية.

أنّ المواقع الالكترونية التي يزورها المتصفح قادرة بدورها على تحديد حركته فيها، وذلك من خلال إدخال ملفات صغيرة تعرف باسم «Cookies» على القرص الصلب (Hard Disk) في جهاز الكومبيوتر. وبالإضافة إلى ذلك، فإنّ المنتديات الالكترونية ومواقع التواصل الاجتماعي، وأهمها» فيسبوك» و«تويتر»، غالباً ما تتضمن ثغرات تمكّن المتطفلين من الاطلاع على أدق التفاصيل الشخصية للمشتركين فيها، وإن كانت هذه المواقع تعمل باستمرار على ابتكار سبل لحماية الخصوصية.

أما الاختراق(Hacking) ، فيمثّل التحدّي الأكبر الذي يواجه الأفراد والشركات والمواقع الالكترونية، وهو يبدو أشبه بحرب مفتوحة لا قاعدة ثابتة لها سوى استفادة كل طرف من ثغرات الطرف الآخر. وهي تتم عادة عبر برامج معقدة وأشكال مختلفة، قد تصل إلى حد رصد تحركاتنا الشخصية، عبر اختراق أجهزة الكومبيوتر المحمولة، وربما مراقبتنا داخل منازلنا.

ففي العالم الرقمي وعالم شبكات المعلومات العالمية ، يترك المستخدم آثار ودلالات كثيرة تتصل به بشكل سجلات رقمية حول الموقع الذي زاره والوقت الذي قضاه على الشبكة والامور التي بحث عنها والمواد التي قام

بتنزيلها والوسائل التي ارسلها والخدمات والبضائع التي قام بطلبها وشرائها انها سجلات تتضمن تفاصيل دقيقه عن شخصية وحياة وهوايات وميول المستخدم على الشبكة وهي سجلات مؤتمتة ذات محتوى شخصي يتصل بالفرد.

والتصفح والتجول عبر الإنترنت يترك لدى الموقع المزار كمية واسعة من المعلومات على الرغم من ان جزءا من هذه المعلومات لازم لاتاحة الربط بالإنترنت والتصفح، وبمجرد الدخول الى صفحة الموقع فان معلومات معينه تتوفر عن الزبون وهي ما يعرف بمعلومات راس الصفحة (header information) وهي التي يزودها الكمبيوتر المستخدم للكمبيوتر الخادم الذي يستضيف مواقع الإنترنت، وهذه المعلومات قد تتضمن :

1. عنوان بروتوكول الإنترنت العائد للزبون (IP) ومن خلاله يمكن تحديد اسم النطاق وتبعا له تحديد اسم الشركة او الجهة التي قامت بتسجيل النطاق عن طريق نظام أسماء المنظمات وتحديد موقعها.
2. المعلومات الأساسية عن المتصفح ونظام التشغيل وتجهيزات النظام المادية المستخدمة من قبل الزبون.
3. وقت وتاريخ زيارة الموقع.
4. مواقع الإنترنت وعنوان الصفحات السابقة التي زارها المستخدم قبل دخوله الصفحة في كل الزيارة.
5. وقد تتضمن أيضاً معلومات محرك البحث الذي استخدمه المستخدم للوصول الي الصفحه، وتبعاً لنوعالمتصفح قد يظهر عنوان البريد الإلكتروني للمستخدم.
6. وايضاً تبعاً لتشغيل المستخدم أوامر خاصة حول ادارة التعامل مع الشبكة قد تظهر معلومات حول الوقت الذي تم قضاؤه في كل صفحة وبيان المعلومات التي ارسلت واستقبلت.

أن العديد ان لم يكن كافة المواقع التفاعليه وتحديداً مواقع النشاط التجاري والتجارة الالكترونية على الانترنت، تتطلب من المستخدم تقديم وتعبئة نموذج يتضمن معلومات مختلفة ، سواء أكان في معرض الاشتراك بخدمات معينة او التسجيل او الانضمام لمجموعات النقاش او حتى لاجراء تعليق او ارسال رسالة. وتتضمن مادة هذه المعلومات اسم المستخدم وعنوانه للعمل والمنزل وارقام الهاتف والفاكس وعنوان البريد الالكتروني ومعلومات حول السن والجنس والحالة الاجتماعية ومكان الاقامة والدخل الشهري او السنوي واحياناً اهتمامات الشخص، واما مواقع البيع والشراء على الانترنت والمواقع التي يتم فيها اجراء عمليات دفع فانها تتطلب رقم بطاقة الاعتماد ونوعها وتاريخ انتهائها.

وبالرغم من المنافع الكبيرة التي أفرزتها تكنولوجيا المعلومات وشبكات المعلومات العالميه فانها ايضاً اوجدت خطراً حقيقياً تمثل بامكانيه جمع المعلومات وتخزينها والاتصال بها والوصول اليها، وجعلها متاحه على الخط قابلة للاستخدام من قبل مختلف قطاعات الاعمال والاجهزة الخلوية بدون علم أو معرفة صاحب المعلومات.

يقول جيري بيرن Jerry Berman وديردري موليغان Deirdre Mulligan ،" تصور انك تسير في احد مخازن الاسواق بين مخازن عديدة لا تعرف ايا منها ، فتوضع على ظهرك اشارة تبين كل محل زرته وما الذي قمت به وما اشتريته ، ان هذا شيء شبيه لما يمكن ان يحصل في بيئة الانترنت [8].

عندما يستخدم الافراد مواقع الانترنت فانهم يتوقعون قدرا من الخفية في نشاطهم اكثر مما يتوقعون في العالم المادي الواقعي ، ففي الاخير يمكن ملاحظة وجودهم ومراقبتهم من قبل الاخرين، وما لم يكشف الشخص عن بيانات تخصه فانه يعتقد ان احدا لن يعرف من هو او ماذا يفعل، لكن الانترنت عبر نظم الخوادم ونظم ادارة الشبكات

تصنع قدرا كبيرا من المعلومات عند كل وقفة في فضاء الشبكة. وهذه البيانات قد يتم اصطيادها ومعرفتها عن موظفي منشاة ما مثلا – من قبل صاحب العمل عند استخدامه للشبكة او لاشتراكاتهم المربوطة عليها ، وقد تجمع من قبل المواقع المزارة نفسها، وكما قلنا فان جمع شتات معلومات وسلوكيات معينة قد يقدم اوضح صورة عن شخص لم يرد كشف اي من تفاصيل ما تضمنته.

ولا توجد في العراق نصوص قانونية خاصة بموضوع حماية الخصوصية الفردية أو حماية الأفراد من المعالجة الآلية للبيانات، وبالتالي فإن المسألة برمتها غير منظمة بعد، ولا يوجد موقف رسمي أو قانوني واضح حيالها.

·ما المقصود بجرائم الكمبيوتر والإنترنت:

توجد عدة تعريفات ومن أهمها:

1. هي نشاط غير مشروع موجه لنسخ أو تغيير أو حذف المعلومات المخزنة داخل الحاسب والتي تحول عن طريقه.
2. هو كل سلوك غير مشروع أو غير مسموح به فيما يتعلق بنقل البيانات.
3. هو نمط من أنماط الجرائم المعروفة في قانون العقوبات طالما مرتبطاً بتقنية المعلومات.
4. هي الجريمة التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دوراً رئيسياً.

·دور الكمبيوتر في الجريمة:

يلعب الكمبيوتر 3 أدوار في ميدان ارتكاب الجرائم وهي:

أولا : قد يكون الكمبيوتر هدفاً للجريمة وذلك كما في حالة الدخول غير المصرح به إلى النظام أو زراعة الفيروسات لتدمير المعطيات والملفات المخزنة أو في حالة الاستيلاء على البيانات المخزنة أو المنقولة عبر النظم.

ثانيا : قد يكون الكمبيوتر أداة الجريمة كما في حالة استغلال الكمبيوتر للاستيلاء على الأموال بإجراء تحويلات غير مشروعة أو استخدام التقنية في عمليات التزييف أو التزوير أو الاستيلاء على الأموال بواسطة أرقام بطاقات الائتمان.

ثالثا : قد يكون الكمبيوتر بيئة الجريمة وذلك كما في تخزين البرامج في نظامه أو في حالة استخدامه لنشر المواد غير القانونية ، ويمكن للكمبيوتر أن يلعب الأدوار الثلاثة معاً.

. الاحتيال وسرقة كلمات المرور:

يمكن حدوث مشاكل عديدة إذا سرق شخص ما كلمة المرور فيمكن لمن يسرق كلمة المرور القيام بأعمال كثيرة منها:

1. قد يستخدم بطاقة الائتمان الخاصة بك لشراء بضائع بآلاف الدولارات عبر الإنترنت.
2. قد يدخل شخص ما إلى مناطق خاصة في مواقع الويب التي قمت بالتسجيل فيها.
3. قد يطلع شخص ما على بريدك الإلكتروني ويقوم بإرسال رسائل تهديد عن طريق بريدك الإلكتروني.
4. قد يستخدم شخص ما حسابك لشن هجمات احتيال على جميع أنحاء العالم وقد يظن الناس انك الفاعل.

·كيف يسرق المحتالون كلمات المرور:

توجد طرق كثيرة لسرقة Password وهي :

1. من أبسط الوسائل التي يستخدمها المحتالون لسرقة كلمة المرور هو أن يتصل بك مدعين أنهم خبراء في أمن الكمبيوتر ويسألون عن كلمة المرور.
2. ومن الوسائل الشائعة أيضاً هي التخمين مثل الحروف الأولى من أسمائهم أو تاريخ ميلاد أحد أقاربهم.
3. الوسيلة الأخيرة وهي التلمس أي محاولة الاكتشاف ويقوم المحتالون بفحص المعلومات التي تعرض عبر الإنترنت وتمكنهم من معرفة كلمة المرور واستخدامها.

المحور الثالث: حماية الخصوصية

حماية الخصوصية المعلوماتية

تمهيد

ان الخصوصية احد حقوق الانسان الاساسية الذي اثار جدلا واسعا على المدى التاريخي، ولعله الحق الذي يعاد التركيز عليه على نحو متعاظم في الوقت الحاضر في ظل افرازات وآثار توظيف تقنية المعلومات.

والخصوصية حق معترف به او ببعض مظاهره او مكوناته في الكتب السماوية، ومعترف به في عدد غير قليل من التشريعات القديمة، اضافة الى اثارته منذ القرن التاسع عشر في العديد من احكام المحاكم. وفي العصر الحديث، اعترف بهذا الحق الاعلان العالمي لحقوق الانسان والعهد الدولي للحقوق المدنية والسياسية واتفاقية حقوق الانسان الاوروبية والاتفاقية الأمريكية لحقوق الإنسان وغيرها.

وللخصوصية وفق تطورها التاريخي ثلاث محطات رئيسة، الاولى :- الاعتراف بالخصوصية كحق لحماية الافراد من مظاهر الاعتداء المادي على حياتهم وممتلكاتهم، وهي ما تعرف بالخصوصية المادية. والثانية :- انطواء الخصوصية على حماية القيم والعناصر المعنوية للشخص، وهي ما عرف بالخصوصية المعنوية. والثالثة الخصوصية كحق عام يمتد نطاقه لحماية الشخص من كافة اوجه الاعتداءات والتدخل في حياته ايا كان مظهرها او طبيعتها، وفي نطاق المعنى الاخير، ولد مفهوم جديد للخصوصية ارتبط باثر التقنية على الحياة الخاصة، تمثل بخصوصية المعلومات او حق الافراد في السيطرة على المعلومات والبيانات الخاصة في مواجهة تحديات العصر الرقمي.

ويمكننا القول ان كافة دول العالم على وجه التقريب أقرت بشكل او بآخر الحق في الخصوصية في واحد او اكثر من مظاهره، وهذا لا يعني توفر حماية كافية، او شمولية في الحماية لدى كافة الدول، وفي الوقت الذي قد نجد فيه حماية الخصوصية بمفهومها المادي اكثر شيوعا واتساعا، تضيق حماية خصوصية المعلومات، وفي ذات الوقت نجدها الشغل الشاغل في الوقت الحاضر للمؤسسات التشريعية ومؤسسات القرار في العديد من دول العالم. اذن فقد تطور الحق في الخصوصية وحماية البيانات في الستينات والسبعينات نتيجة للتأثر بتقنية المعلومات وبسبب القوى الرقابية المحتملة لانظمة الكمبيوتر التي استوجبت وضع قواعد معينة تحكم جمع ومعالجة البيانات الخاصة، وفي هذا الحقل فان من المهم الاشارة الى ان اول معالجة تشريعية في ميدان حماية البيانات كان عام 1970 في

ولاية هيس بالمانيا (LAND OF HESSE IN GERMANY)، لكن هذه المعالجة لا تعد قانونا متكاملا لاعتبارات عديدة اولها انه ليس قانون دولة، وقد تبعه سن اول قانون وطني (متكامل) في السويد عام 1973 ثم الولايات المتحدة عام 1974 ثم المانيا على المستوى الفدرالي عام 1977 ثم فرنسا عام 1978.

وفي عام 1981 وضع مجلس أوروبا اتفاقية حماية الافراد من مخاطر المعالجة الالية للبيانات الشخصية، ووضعت كذلك منظمة التعاون الاقتصادي والتنمية دليلا ارشاديا لحماية الخصوصية ونقل البيانات الخاصة، والذي قرر مجموعة قواعد تحكم عمليات المعالجة الإلكترونية للبيانات، وهذه القواعد تصف البيانات والمعلومات الشخصية على انها معطيات تتوفر لها الحماية في كل مرحلة من مراحل الجمع COLLECTION والتخزين STORAGE والمعالجة PROCESSING والنشر DISSEMINATION. ثم وفي خطوة متطورة على المستوى التشريعي الاقليمي، بل وذات اثر عالميا، اصدر الاتحاد الأوروبي الامر التشريعي الخاص بحماية البيانات ونقلها عبر الحدود لعام 1995، الذي مثل مرحلة جديدة في اعادة تنظيم خصوصية المعلومات ادت الى اعادة وضع العديد من دول أوروبا تشريعات جديدة او تطوير تشريعاتها القائمة في هذا الحقل، بل اثر فيما تضمنه من معايير في حقل نقل البيانات خارج الحدود لجهة سعي العديد من دول العالم خارج نطاق اوروبا الى التواؤم مع ما قرره هذا القانون، وبالعموم يمكننا القول بإيجاز ان مفهوم حماية البيانات في المواثيق المتقدمة يتطلب ان تكون البيانات الشخصية :-

1 – قد تم الحصول عليها بطريق مشروع وقانوني.

2 – تستخدم للغرض الأصلي المعلن والمحدد ولا تكشف لغير المصرح لهم بالاطلاع عليها.

3 – تتصل بالغرض المقصود من الجمع ولا تتجاوزه ومحصورة بذلك.

4 – صحيحة وتخضع لعمليات التحديث والتصحيح.

5 – يتوفر حق الوصول اليها مع حق الإخطار بأنشطة المعالجة او النقل وحق التصحيح والتعديل وحتى طلب الالغاء.

6 – تحفظ سرية وتحمى سريتها وفق معايير امن ملائمة لحماية المعلومات ونظم المعالجة.

7 – تتلف عند استنفاذ الغرض من جمعها.

وقد شهدت الستينات انطلاق الاهتمام بحماية الخصوصية من مخاطر التكنولوجيات الحديثة، لينطلق معه مفهوم حماية البيانات الخاصة من مخاطر التقنية، ومنذ مطلع السبعينات بدأت دول العالم تتبنى قوانين حماية الخصوصية اما عن طريق القوانين الشمولية التي تعترف بالحق وتقر المبادئ الأساسية وتقدم الاطار القانوني الموضوعي والإجرائي لحماية خصوصية المعلومات او حماية البيانات التي تتصل بالافراد وحياتهم الخاصة (البيانات الشخصية)، او عن طريق حزمة قوانين قطاعية تتعلق بالبيانات في قطاعات معينة، كالبيانات الصحية او المالية او بيانات الاحوال المدنية او غيرها، الى جانب مدونات سلوك تحكم قطاعات معينة كقطاعات الصناعة او الخدمات التقنية فيما يعرف بوسيلة التنظيم القانوني الذاتي للقطاعات او السوق. وغالبية هذه القوانين ان لم تكن كلها اعتمدت في محتواها وما تضمنته على قرارات مجلس أوروبا عامي 73 و74 واتفاقية (مجلس اوروبا) الخاصة بحماية البيانات من مخاطر المعالجة الآلية لعام 1980، وعلى دليل منظمة التعاون الاقتصادي والتنمية لعام

1980 ودليل الامم المتحدة اللاحق عام 1990، وفي تطورها وشموليتها خلال السنوات الخمس الأخيرة اعتمدت بشكل واضح على تعليمات (الامر التشريعي) للاتحاد الأوروبي لحماية البيانات عام 1995، وقد مثلت قواعد هذه المدونات ما يمكن تسميته الشرعة الدولية لحماية البيانات أو دستور خصوصية المعلومات. وهي تسمية نطلقها في هذه المرحلة من تطور موضوع خصوصية المعلومات لما لمسناه من اثر حقيقي لها في صياغة النظام القانوني لحماية البيانات والخصوصية في العصر الرقمي.

وبالعودة للأمر التشريعي بشأن حماية البيانات الصادر عن الاتحاد الأوروبي عام 1995، وفي نقلة نوعية مثلت تكريسا لمفهوم خصوصية المعلومات واقامة التوازن بين هذا الحق والحق في تدفق المعلومات عبر الحدود ومواجهة تحديات توظيف التكنولوجيا في الانشطة الادارية والانتاجية والخدمية في الدولة، اصدر الاتحاد الاوروبي في عام 1995 دليلا شاملا – ملزما لدول الاتحاد الاوروبي ، ولهذا نطلق عليه الأمر التشريعي ويسميه البعض قانونا او تعليمات – يتعلق بحماية خصوصية المعلومات وتنظيم نقل المعلومات خارج الحدود، وقد اقر من قبل البرلمان الاوروبي ومجلس اوروبا معا، وتبعه عام 1997 دليل اخر لتنظيم معالجة البيانات الشخصية في قطاع الاتصالات، وهذا الجهد الجديد – مضافا اليه استمرار الجهود من قبل اطر الامم المتحدة ومؤسسات اوروبا الموحدة ومنظمة التعاون الاقتصادي والتنمية عبر اصدار ادلة متعددة تعالج مختلف طوائف البيانات وحمايتها في البيئة الرقمية – جاء معتمدا على النشاط السابق الذي انتج المدونات المشار اليها اعلاه، وتميز الامر التشريعي للاتحاد الاوروبي لعام 1995 بالزام الدول الاوروبية بإدماجه ضمن تشريعاتها في فترة أقصاها نهاية أكتوبر 1998، وهو ما ادى الى موجة تشريعية جديدة وموجة تعديل التدابير التشريعية القائمة في مختلف دول اوروبا، وتحديدا الدول الخمسة عشر الأعضاء في الاتحاد، واثر ذلك على عشرات دول العالم من خارج اوروبا التي وجدت في هذه التجربة الناضجة لحماية البيانات الشخصية هاديا لها ونموذجا متقدما امكنها الاعتماد عليه لاقرار تشريعات حماية البيانات الشخصية او تشريعات الخصوصية الشمولية في دولها.

ولان التوازن بين الحق في حماية البيانات الخاصة وفق مبادئ الخصوصية المتصلة بانشطة جمع ومعالجة وكشف هذه البيانات، وبين الحق في الوصول للمعلومات، يتطلب اقرار معيار توازن مقبول لان الخصوصية في حقيقتها قيد على حق الوصول للمعلومات، وهذا ادى الى اعادة دراسة التجربتين وتقييمهما معا من قبل هيئات حماية البيانات الشخصية وجهات المعلوماتية في النظم المقارنة، واصبح خير موضع لبحثهما الجهات ذات العلاقة بمسائل المعلوماتية او تقنية المعلومات او الجهات المعنية بسياسات المعلومات والكمبيوتر والاتصالات، واتجهت غالبية الدول الى اقرار التشريعات في الحقلين كل على استقلال، في حين اتجهت دول مثل هنجاريا الى تنظيم الحقين في تشريع واحد، من اجل ضمان سلامة معيار التوازن بين الحق في المعلومات والحق في الخصوصية وانعكاسه على نحو صحيح في الاحكام التفصيلية التي تنظم ممارسة كلا الحقين. وساهم في ذلك ان الامر التشريعي الأوروبي لعام 1995 نظم حماية البيانات الشخصية وبنفس الوقت الحق في نقل البيانات خارج الحدود وهو جزء من مسائل الحق في الوصول للمعلومات، ووجدت بعض الدول، حتى مع وجود التشريعين كل على استقلال، ان الجهة المعنية باحكامهما معا يتعين ان تكون جهة واحدة، لهذا مثلا نجد توجها لاناطة صلاحيات مراقبة ومتابعة مسائل الحق في الوصول للمعلومات لجهات (مفوضي) حماية البيانات المنشأة بموجب قوانين حماية

البيانات، كما هو الشأن في بريطانيا، فقد قامت بريطانيا عام 1998 بتسمية جهة الرقابة على حماية البيانات الشخصية بمفوض حماية البيانات في اعقاب قانون حماية البيانات البريطاني لعام 1998 (وكذلك صدور قانون حقوق الانسان البريطاني عام 1998) بدل مفوض تسجيل البيانات الذي أنشي بموجب قانون حماية البيانات عام 1984 وبصدور قانون حرية المعلومات البريطاني لعام 2000 ايضا، جرى تعديل قانون حماية البيانات لعام 1998 في مسائل عديدة منها اعادة تسمية مفوض حماية البيانات ومحكمة البيانات المنشأتين بموجب قانون 1998 ليصبحا مفوض المعلومات، ومحكمة المعلومات، مسندة لهما اختصاصات تتعلق بالحقين معا:- حماية البيانات الشخصية (الخصوصية) وحرية المعلومات (الحق في الوصول للمعلومات والسجلات) وهو توجه اريد منه ايجاد جهة واحدة تباشر مهام متعددة بالنسبة المعلومات، سواء حق الوصول اليها او حق حظر المساس بالبيانات الشخصية منها لضمان عدم اختلال معيار التوازن لدى مباشرة الحقين.

اذا يمكننا القول ان خصوصية المعلومات هي حماية البيانات ، لكن الخصوصية ليست هي حماية البيانات، فالاخيرة شيء من الخصوصية وتتعلق بمواجهة الاعتداءات على البيانات الشخصية وتنظيم الحق في البيانات الشخصية وسيطرة صاحبها عليها، في حين ان الخصوصية على اطلاقها ، تنطوي على خصوصية البيانات، وخصوصية الاتصالات في مواجهة انشطة الرقابة والتجسس، وخصوصية المكان وحرمته في مواجهة انشطة الاعتداء المادية، وهي مسائل حرمة المسكن وحرمة الشخص من التفتيش غير القانوني، وايضا خصوصية المراسلات ومن ضمنها مراسلات مادية واخرى الكترونية، وغير ذلك من اوجه الحماية ذات الطبيعة او المحتوى المادي او المعنوي، ولا يعني قولنا هذا تقسيم الحق في الخصوصية، فهو بوصفه الحق الذي تحمى فيه حياة الفرد الخاصة من كل اعتداء وتطاول وانتهاك او تدخل، مادي او معنوي، ولهذا فهو يشمل هذه المظاهر وغيرها دون ان ينتقص ذلك من كونه حقا موحدا مستقلا. فالخصوصية بالعموم تنطوي على حماية مظاهر مادية ومعنوية ومعلوماتية – ان جاز التعبير – ولا تقف عند حماية البيانات الشخصية، وبالتالي من المهم ان ندرك ان الترادف بوجه عام قائم ما بين اصطلاح خصوصية المعلومات وحماية البيانات، وليس بين الخصوصية وبين حماية البيانات، اما شيوع استخدام اصطلاح الخصوصية مستقلا ومنفردا دون الحاقه بالبيانات في البيئة الإلكترونية للدلالة على حماية البيانات واستخدامه كذلك في الدراسات الأكاديمية وفي الدراسات التقنية وأبحاث وتقرير قطاعات الأعمال، فهو امر يرجع الى ان تعبير الخصوصية شاع بوقعه هذا في ظل تزايد مخاطر التقنية الى مدى ارتبط بها في الاستخدام وكأنه ينحصر في نطاقها وبيئتها، وهو طبعا ليس بكذلك ، لكن ربما لان اشد ما يمكن ان يمثل تغولا على هذا الحق وانتهاكا له، هو الوسائل التقنية ومخاطر المعالجة الآلية للبيانات. كما ان استخدام اصطلاح الخصوصية في بيئة مواقع الإنترنت ومسائل عقود التقنية او خدمات التقنية عموما يشير الى حماية الخصوصية المعلوماتية او حماية البيانات.

دور تقنية المعلومات في حماية الخصوصية المعلوماتية[16]

ان التطورات الحديثة في تقنية المعلومات أحدثت تغيرات مستمرة ومضطردة في اساليب العمل والميادين كافة، اذ أصبحت عملية انتقال المعلومات عبر الشبكات المحلية والدولية وأجهزة الحاسوب من الامور الروتينية في عصرنا

الحالي واحدى علامات العصر المميزة التي لا يمكن الاستغناء عنها لتأثيرها الواضح في تسهيل متطلبات الحياة العصرية من خلال تقليل حجم الاعمال وتطوير اساليب خزن وتوفير المعلومات حيث أن انتشار انظمة المعلومات المحوسبة أدى الى ان تكون عرضة للاختراق لذلك أصبحت هذه التقنية سلاحا ذو حدين تحرص المنظمات على اقتناءه وتوفير سبل الحماية له.

أن موضوع الامن المعلوماتي يرتبط أرتباطا وثيقا بامن الحاسوب فلا يوجد امن للمعلومات اذا لم يراعى أمن الحاسوب، وفي ظل التطورات المتسارعة في العالم والتي اثرت على الامكانات التقنية المتقدمة المتاحة والرامية الى خرق منظومات الحاسوب بهدف السرقة او تخريب المعلومات او تدمير احهزة الحاسوب، كان لا بد من التفكير الجدي لتحديد الاجراءات الدفاعية والوقائية وحسب الامكانات المتوفرة لحمايتها من اي اختراق او تخريب، وكان على ادارة المنظمات ان تتحمل مسؤولية ضمان خلق اجواء أمنية للمعلومات تضمن الحفاظ عليها.

أصبحت خصوصية البيانات (أو المعلومات) إحدى حقول البحث متزايدة الأهمية في عصرنا الحالي –عصر تقنية المعلومات، خاصة في إدارة بيانات المؤسسات والإدارات الحكومية وكذلك الشركات الخاصة التجارية والخدمية والصحية، تلك التي تقوم بتخزين مئات الآلاف أو الملايين من سجلات العملاء أو المواطنين، والتي تتضمن بياناتهم الشخصية واهتماماتهم والأنشطة التي قاموا بها وميولهم، مع الإمكانية الجبارة في تحليل هذه البيانات ومقارنتها وسهولة نقلها بين القارات في ثواني معدودة. وبتصاعد عدد المخترقين (Hackers) و سارقي الهويات (Theft Identity)، فعمليات اختراق خصوصية البيانات تقوم بالتأثير على حياتنا الخاصة وأعمالنا بشكل لم نكن لنتخيله من قبل. فوفقاً لتقرير منظمة (PRC Privacy Rights – Clearinghouse)، أنه منذ شهر يناير 2005 إلى سبتمبر 2008، فإن عدد السجلات التي تحتوي على معلومات شخصية حساسة وتم اختراقها أمنياً في الولايات المتحدة فقط تجاوزت 230,411,730 سجل، والعدد في ازدياد يومي.

إن من أكثر التحديات صعوبة في إدارة أمن البيانات الخصوصية هي الامتثال للأنظمة، حيث قامت مؤخراً – في نوفمبر 2008– مؤسسة أي.م.ر للبحوث (Ltd AMR Research.) باستطلاع شمل 154 متخذ قرار في كبرى شركات تقنية المعلومات في الولايات المتحدة الأمريكية. استخلص البحث أن أكثر ثلاث صعوبات في إدارة خصوصية البيانات هي: تعدد واختلاف سياسات الخصوصية في المناطق المختلفة –جغرافياً، ومواكبة التغييرات المستمرة في الأنظمة والسياسات، وأخيراً إجبار الأفراد والمنشآت الحكومية لإتباع هذه القوانين والأنظمة. واستُنتِج أيضاً، بأن أكثر ما يخشى عليه أصحاب الشركات في قضايا خصوصية البيانات هي خسارة ثقة العملاء و الموظفين والمستثمرين والعلامات التجارية، ثم يأتي خشية فقدان الحقوق الفكرية للمنتجات والبحوث والدراسات، ومن ثم يأتي الخوف من التلاعب بالحسابات المالية للمنشأة. والجدير بالذكر أن 55% من الشركات المشاركة في الاستطلاع ستقوم بزيادة قيمة الاستثمار الداخلي في قضايا حفظ خصوصية البيانات في عام 2009 مقارنة بما أنفقته في العام الأسبق، وتتمثل هذه الزيادة باستخدام التقنيات والسياسات الحديثة مثل: أمن الشبكات (من جدران نارية ومضادات الفيروسات والشبكات الخاصة الافتراضية VPN)، وأدوات مراقبة أنشطة قواعد البيانات، والأمن الاحترازي (من أنظمة كشف التلاعب وكشف نقاط ضعف التطبيقات والشبكات)، وتطبيقات الحكم والخطورة والإذعان (GRC)، وغيرها من الأنظمة والأدوات التي تساعد المنشآت في حماية خصوصية بياناتها.

وأخيراً فإن القلق المتزايد من الناس حول حفظ خصوصياتهم يجب أن يكون رد فعل لطريقة استخدام المنشآت لتلك المعلومات وليس لتقنية المعلومات بذاتها"، فالتقنية سلاح ذو حدين والمستخدم هو من يحدد أي الحدين يستخدم. وللحفاظ على خصوصيتك وخصوصية بياناتك هذه بعض النصائح، قم بقراءة سياسات الخصوصية (Privacy Policy) قبل تسجيل أي بيانات خاصة بك في مواقع الانترنت، وكن حذر دائماً عند تسجيل البيانات الخصوصية. تأكد من أن الموقع يستخدم إحدى تقنيات التشفير، ويمكن معرفة ذلك من عنوان الموقع (Address URL)، مثلاً أن يبدأ العنوان بـ https، وتأكد من وجود علامة القفل في زاوية الشاشة. قم بقراءة اتفاقيات الاستخدام قبل تنصيب البرامج. قم بفحص دوري للبرامج التي تعمل في جهازك وتستخدم إحدى المنافذ لديك للاتصال بشبكة الانترنت وذلك بتنفيذ الأمر التالي (Netstat <– Run <– Start)، أو باستخدام أحد برامج مراقبة المنافذ مثل البرنامج المجاني Distroy Spybot Search and. لا تقم بالاتصال بالانترنت باستخدام شبكة لاسلكية مجهولة أو أنها لا تستخدم إحدى بروتوكولات الحماية الحديثة مثل WPA2. قم بتغيير الإعدادات الافتراضية المستخدمة من الشركة المصنعة، مثل اسم الجهاز وكلمات المرور. قم بتبليغ الجهات المختصة عند اكتشافك لمواقع مشبوهة، وعند تعرض جهازك لأي اختراق أمني و تسرب معلومات خاصة عنك أو عن عملائك.

ما هي المعلومات الرئيسة المتصلة بامن المعلومات[17]؟

تتعدد عمليات التعامل مع المعلومات في بيئة النظم وتقنيات المعالجة والاتصال وتبادل البيانات، ولكن يمكن بوجه عام تحديد العمليات الرئيسة الاتية:

١. تصنيف المعلومات Information classification

وهي عملية اساسية لدى بناء اي نشاط يتعلق بالمعلومات وتختلف التصنيفات حسب المنشاة، فمثلا قد تصنف المعلومات الى معلومات متاحة، وموثوقة، وسرية، وسرية للغاية، او قد تكون معلومات متاح الوصول اليها واخرى محظور التوصل اليها وهكذا.

٢. التوثيق Documentation

وتتطلب عمليات المعلومات اساسا اتباع نظام توثيق خطي لتوثيق بناء النظام وكافة وسائل المعالجة والتبادل ومكوناتها. وبشكل رئيس فان التوثيق لازم وضروري لنظام التعريف والتخويل، وتصنيف المعلومات ،والانظمة التطبيقية، وفي اطار الامن، فان التوثيق يتطلب ان تكون استراتيجية او سياسة الامن موثقة ومكتوبة وان تكون اجراءاتها ومكوناتها كاملة، فضلا عن خطط التعامل مع المخاطر والحوادث، والجهات المسؤولة ومسؤولياتها وخطط التعافي وادارة الازمات وخطط الطوارئ المرتبطة بالنظام عند حدوث الخطر.

٣. المهام والواجبات الادارية والشخصية Administration and Personnel Responsibilities

ان مهام المتصلين بنظام أمن المعلومات تبدا في الاساس من حسن اختيار الافراد المؤهلين وعمق معارفهم النظرية والعملية، على ان يكون مدركا ان التاهيل العلمي يتطلب تدريبا متواصلا ولا يقف عند حدود معرفة وخبرة هؤلاء لدى تعيينهم، وبشكل رئيس فان المهام الادارية او التنظيمية تتكون من خمسة عناصر او

مجموعات رئيسة وهي (تحليل المخاطر، وضع السياسة او الاستراتيجية، وضع الامن، وضع البناء التقني الامني – توظيف الاجهزة والمعدات والوسائل، واخيرا تنفيذ الخطط والسياسات). ومن المهم ادراك ان نجاح الواجبات الادارية او الجماعية للمنشاة يتوقف على ادراك كافة المعنيين في الادارة(بمهامهم التقنية والادارية والمالية) باستراتيجية وخطة وواجبات الامن والتزام المؤسسة باعتبار مسائل الامن واحدا من الموضوعات التي يدركها الكافة ويتمكن الكل من التعامل مع ما يخص واجباتهم من بين عناصر الامن. وعلى المستوى الشخصي او مستوى المستخدمين، فان على المؤسسة ان تضع التوجيهات الكافية لضمان وعي عام ودقيق بمسائل الامن، بل المطلوب بناء ثقافة الامن لدى العاملين والتي تتوزع بين وجوب مراعاة اخلاقيات استخدام التقنية وبين الاجراءات المتطلبة من الكل لدى ملاحظة اي خلل، وعلى المؤسسة ان تحدد للمستخدمين ما يتعين عليهم القيام به والاهم ما يحظر عليهم القيام به في معرض استخدامهم للوسائل التقنية المختلفة.

٤. وسائل التعريف والتوثيق من المستخدمين وحدود صلاحيات الاستخدام Identification and Authorization

ان الدخول الى انظمة الكومبيوتر وقواعد البيانات ومواقع المعلوماتية عموما، يمكن تقييده بالعديد من وسائل التعرف على شخصية المستخدم وتحديد نطاق الاستخدام، وهو ما يعرف بانظمة التعريف والتخويل Identification and Authorization system والتعريف او الهوية مسالة تتكون من خطوتين، الاولى وسيلة التعرف على شخص المستخدم والثانية قبول وسيلة التعريف او ما يسمى التوثيق من صحة الهوية المقدمة. ووسائل التعريف تختلف تبعا للتقنية المستخدمة، وهي نفسها وسائل أمن الوصول الى المعلومات او الخدمات في قطاعات استخدام النظم او الشبكات او قطاعات الاعمال الالكترونية، وبشكل عام فان هذه الوسائل تتوزع الى ثلاثة انواع وكما ياتي:

أ. شيئ ما يملكه الشخص مثل البطاقة البلاستيكية او غير ذلك.

ب. شيئ ما يعرفه الشخص مثل كلمات السر او الرمز او الرقم الشخصي وغير ذلك.

ت. شيئ ما يرتبط بذات الشخص او موجود فيه مثل بصمة الاصبع او بصمة العين والصوت وغيرها.

٥. عمليات الحفظ Back-up

وعمليات الحفظ تتعلق بعمل نسخة اضافية من المواد المخزنة على احدى وسائط التخزين سواء داخل النظام او خارجه. وتخضع عمليات الحفظ لقواعد يتعين ان تكون محددة سلفا وموثقة ومكتوبة ويجري الالتزام بها لضمان توحيد معايير الحفظ وحماية النسخ الاحتياطية، ويمثل وقت الحفظ، وحماية النسخة الاحتياط، ونظام الترقيم والتبويب، وآلية الاسترجاع والاستخدام، ومكان الحفظ وأمنه، وتشفير النسخ التي تحتوي معطيات خاصة وسرية/ مسائل رئيسية يتعين اتخاذ معايير واضحة ومحددة بشانها.

٦. وسائل الامن الفنية ونظام منع الاختراق

تتعدد وسائل الامن التقنية المتعين استخدامها في بيئة الكومبيوتر والانترنت، كما تتعدد اغراضها ونطاقات الاستخدام، وقد تناولنا فيما تقدم مسائل التعريف والتوثيق وتحديدا كلمات السر ووسائل التعريف الاخرى، وتتخذ التشفيرات Cryptography ، وكذلك نظم التحكم في الدخول، ونظام تحري الاختراق Intrusion

Detection systems، وانظمة وبرمجيات مقاومة الفيروسات أهمية متزايدة، لكنها لا تمثل جميعها وسائل الامن المستخدمة، بل هي اضافة لوسائل التعريف والتوثيق المتقدم الاشارة اليها تمثل اهم وسائل الامن التقنية في الوقت الحاضر.

مفهوم الامن المعلوماتي وحماية الخصوصية المعلوماتية على شبكة الانترنت[18]

تشكل المعلومات في المنظمات البنية التحتية التي تمكنها من اداء مهامها، اذ ان نوع المعلومات وكميتها وطريقة عرضها تعتبر الاساس في نجاح صنع القرارات داخل المنظمات المعاصرة وعليه فان للمعلومات قيمة عالية تستوجب وضع الضوابط اللازمة لاستخدامها وتداولها ووضع السبل الكفيلة بحيازتها، لذا فان المشكلة التي يجب اخذها بالحسبان هو توفير الحماية اللازمة للمعلومات وابعادها عن الاستخدام غير المشروع لها. فقد عرف أمن المعلومات بانه مجموعة من التدابير الوقائية المستخدمة في المجالين الاداري والفني لحماية مصادر البيانات من اجهزة وبرمجيات وبيانات من التجاوزات او التدخلات غير المشروعة التي تقع عن طريق الصدفة او عمدا عن طريق التسلل او الاجراءات الخاطئة المستخدمة من قبل ادارة المصادر المعلوماتية، فضلا عن اجراءات مواجهة الاخطار الناتجة عن الكوارث الطبيعية المحتملة التي تؤدي ومن ثم التاثير على نوع ومستوى الخدمة المقدمة.

ويمكن تعريف أمن المعلومات من زاوية اكاديمية، هو العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن انشطة الاعتداء عليها. ومن زاوية تقنية، هو الوسائل والادوات والاجراءات اللازم توفيرها لضمان حماية المعلومات من الاخطار الداخلية والخارجية. ومن زاوية قانونية، فان أمن المعلومات هو محل دراسة وتدابير حماية سرية وسلامة محتوى وتوفر المعلومات ومكافحة انشطة الاعتداء عليها او استغلال نظمها في ارتكاب الجريمة، وهو هدف وغرض تشريعات حماية المعلومات من الانشطة غير المشروعة وغير القانونية التي تستهدف المعلومات ونظمها(جرائم الكمبيوتر والانترنت).

أن مفهوم الامن المعلوماتي مر بمراحل تطويرية عدة أدت الى ظهور ما يسمى بأمنية المعلومات، ففي الستينات كانت الحواسيب هي كل ما يشغل العاملين في أقسام المعلومات، وكان همهم هو كيفية تنفيذ البرامج والايعازات ولم يكونوا مشغولين بأمن المعلومات بقدر انشغالهم بعمل الاجهزة وكان مفهوم الامنية يدور حول تحديد الوصول او الاطلاع على البيانات من خلال منع الغرباء الخارجين من التلاعب في الاجهزة لذلك ظهر مصطلح أمن الحواسيب والذي يعني حماية الحواسيب وقواعد البيانات، ونتيجة للتوسع في استخدام أجهزة أمن الحاسبات (Computer security) وما تؤديه من منافع تتعلق بالمعالجة للحجوم الكبيرة من البيانات، تغير الاهتمام ليمثل السيطرة على البيانات ورافق ذلك استخدام كلمات أمن البيانات(Data security) وحمايتها. وفي التسعينات تم الانتقال الى مفهوم أمن البيانات، السر البسيط للسيطرة على الوصول للبيانات، أضافة الى وضع اجراءات الحماية لمواقع الحواسيب من الكوارث واعتماد خطط نسخ اضافية من البيانات والبرمجيات بعيدا عن موقع الحاسوب، وفي مرحلة الثمانينات والتسعينات ازدادت أهمية استخدام البيانات، وساهمت التطورات في مجال تكنولوجيا المعلومات بالسماح لاكثر من مستخدم للمشاركة في قواعد البيانات، كل هذا أدى الى الانتقال من مفهوم أمن البيانات الى أمن المعلومات، وأصبح من الضروري المحافظة على المعلومات وتكاملها وتوفرها ودرجة موثوقيتها، حيث أن الاجراءات الامنية المناسبة يمكن ان تساهم في ضمان النتائج المرجوة وتقليص اختراق المعلومات والتلاعب بها.

أن حماية الخصوصية لمستخدم شبكة الانترنت هي جزء من الامن على الشبكة ولكن الامن ليس بالضرورة جزء من حماية الخصوصية، فان مفهوم الامن على الشبكة يمكن ان يتم من خلال قيامك بعدة خطوات وترتيبات فعالة لحماية جهازك ومعلوماتك الهامة وحماية الخصوصية تعتبر جزء من هذه الترتيبات الامنية المتخذة لسلامة جهازك ومعلوماتك ومن هذه الخطوات ما ياتي[19]:.

اولا: التحكم بملفات المشاركة المحلية LAN لان نظام ويندوز يقوم بفتح هذه الملفات بطريقة مباشرة كشئ اساسي في النظام وتعتبر هذه الملفات اكبر مصدر تهديد أمني لك لانها تسمح لاي شخص في الانترنت من الدخول الى جهازك ومشاركتك في ملفاتك ومعلوماتك الموجودة في الجهاز.

ثانيا: أحمي جهازك بمنع الاخرين من الدخول اليه باستخدام جهاز خاص يسمى Smart key .

ثالثا: تجنب تنزيل او تحميل اي برامج او ملفات ذات طبيعة تنفيذية خاصة من مصادر غير موقوق بها.

رابعا: تجنب فتح الملفات المرفقة في الرستئل الالكترونية من مصادر غير معروفة لديك وخاصة اذا كانت من نوع Com, and.bat, exe

خامسا: اذا كنت تملك معلومات في غاية الاهمية او خاصة جدا قم باستخدام اي برنامج لتشفير معلوماتك ورسائلك الالكترونية.

سادسا: لا تقم باي عملية شراء من شبكة الانترنت دون التاكد من استخدام سيرفر أمن ووجود علامة القفل مغلق في المتصفح وكذلك تغير http:// to https.// :

سابعا: تجنب الموافقة على حفظ اسم المستخدم وكلمات العبور لانك لو وافقت على ذلك فسوف تسهل العملية على الهاكرز من الدخول لانه سوف يجدها مخزونة وجاهزة له.

ان اهم العناصر الواجب اتخاذها لتوفير الحماية على اية معلومات ما ياتي:

١. السرية او الموثوقية CONFIDENTIALITY وتعني التأكد من ان المعلومات لا تكشف ولا يطلع عليها من قبل اشخاص غير مخولين بذلك.
٢. التكاملية وسلامة المحتوى INTEGRITY وتعني التاكد من ان محتوى المعلومات صحيح ولم يتم تعديله او العبث به وبشكل خاص لن يتم تدمير المحتوى او تغيره او العبث به في اية مرحلة من مراحل المعالجة او التبادل سواء في مرحلة التعامل الداخلي مع المعلومات او عن طريق تدخل غير مشروع.
٣. استمرارية توفر المعلومات او الخدمة AVAILABILITY ويعنى بالتاكد من استمرار عمل النظام المعلوماتي واستمرار القدرة على التفاعل مع المعلومات وتقديم الخدمة لمواقع المعلوماتية، وان مستخدم المعلومات لن يتعرض الى منع استخدامه لها او دخوله اليها.
٤. عدم انكار التصرف المرتبط بالمعلومات ممن قام به NON REPUDIATION ويقصد به ضمان عدم انكار الشخص الذي قام بتصرف ما متصل بالمعلومات او مواقعها، بحيث تتوفر قدرة اثبات ان تصرفا ما قد تم من شخص ما في وقت معين.
٥. أن ضمان عناصر امن المعلومات كلها او بعضها يعتمد على المعلومات محل الحماية واستخداماتها وعلى الخدمات المتصلة بها، فليس كل المعلومات تتطلب السرية وضمان عدم الافشاء، وليس كل المعلومات بذات الاهمية من حيث الوصول لها او ضمان عدم العبث بها، ولهذا تنطلق خطط أمن المعلومات من الاجابة على سلسلة تساؤلات متتالية[1]:

التساؤل الاول: ما الذي نريد ان نحميه؟ واجابة هذا التساؤل تحدد تصنيف البيانات والمعلومات من حيث أهمية الحماية. اذ تصنف المعلومات تبعا لكل حالة على حدة، من معلومات لا تتطلب حماية، الى معلومات تتطلب حماية قصوى.

التساؤل الثاني: ما هي المخاطر التي تتطلب هكذا حماية؟ وتبدا عملية تحديد المخاطر بتصور كل خطر قد يمس المعلومات محل الحماية او يهدد امنها، ابتداء من قطع الكهرباء عن المبيوتر وحتى مخاطر اختراق النظام من الخارج بواحد او اكثر من وسائل الاختراق عبر نقاط الضعف، مرورا باساءة الموظفين استخدام كلمات السر العائدة لهم، ويصار الى تصنيف هذه المخاطر ضمن قوائم تبعا لاساس التصنيف، فتصنف كمخاطر من حيث مصدرها ومن حيث وسائل تنفيذها، ومن حيث غرض المتسببين بهذه المخاطر، ومن حيث اثرها على نظام الحماية وعلى المعلومات.

التساؤل الثالث: كيف يتم توفير الحماية لما نرغب بحمايته من المخاطر التي تم تحديدها(وسائل الحماية)؟ وهنا نجد كل منشاة وكل هيئة طريقتها الخاصة في توفير الامن من المخاطر محل التحديد وبحدود متطلبات حماية المعلومات المخصوصة التي تم تحديدها وبحدود امكانياتها المادية والميزانية المخصصة للحماية، فلا تكون اجراءات الامن رخوة ضعيفة لا تكفل الحماية وبالمقابل لا تكون مبالغا بها الى حد يؤثر على عنصر الاداء في النظام. ففي بيئة المعلومات فمن الطبيعي مثلا ان نضع على جهاز الكمبيوتر الشخصي كلمة السر للولوج الى الملفات الهامة او حتى للنظام كله وان لا نعطي الكلمة لاحد، وان نضع برنامجا او اكثر لمقاومة الفيروسات الالكترونية الضارة، ونراعي اجراءات مقبولة في حماية الدخول الى شبكة الانترنت والتاكد من مصدر البريد الالكتروني مثلا. فاذا كان الكومبيوتر في دائرة خاصة او منشاة معينة ويضم بيانات هامة ومصنف انها سرية، كان لزاما علينا زيادة الاجراءات الامنية، فمثلا يضاف للنظام جدران نارية تحد من دخول اشخاص من الخارج وتمنع اعتداءات منظمة قد يتعرض لها النظام او الموقع المعلوماتي، واذا كان النظام يتبادل رسائل الكترونية يخشى على بياناتها من الافشاء، تكون هنا تقنيات التشفير مطلوبة بالقدر المناسب. لكن لا يقبل مثلا على جهاز كمبيوتر خاص غير مرتبط بشبكة عامة ان يوضع على احد مواقع الانترنت وسائل تعريف متعددة لشخص المستخدم، ككلمة السر والبصمة الالكترونية والبصمة الصوتية، وان يخضع نظام الموقع الى تشفير طويل المدى لكافة البيانات الموجودة عليه والمتبادله عبره. بمعنى لكل ذلك ان اجراءات الحماية تنطلق من احتياجات الحماية الملاءمة، فان زادت عن حدها امست ذات اثر سلبي على الاداء، فاصبح الموقع او النظام بطيئا وغير فاعل في اداء مهامه الطبيعية، وان نقصت عن الحد المطلوب ازدادت نقاط الضعف واصبح اكثر عرضة للاختراق الداخلي والخارجي.

التساؤل الرابع: ما العمل ان تحققت اي من المخاطر رغم وسائل الحماية؟ والاجابة عن هذا التساؤل هو ما يعرف بخطط مواجهة الاخطار عند حصولها، وتتضمن مراحل متتالية، تبدا من مرحلة الاجراءات التقنية والادارية والاعلامية والقانونية اللازمة عند حصول ذلك، ومرحلة اجراءات التحليل لطبيعة المخاطر التي

حصلت وسبب حصولها وكيفية منع حصولها لاحقا. واخيرا اجراءات التعافي والعودة الى الوضع الطبيعي قبل حصول الخطر مع مراعاة تنفيذ ما اظهره التحليل عن كيفية حصول المخاطر وضمان عدم حصولها.

الهجمات والمخاطر المتصلة بعمليات الحماية المعلوماتية(20)

اذا اردنا ان نوصف المخاطر المتصلة بعمليات الحماية ذاتها ربما نكون في الحقيقة امام كافة انواع المخاطر والهجمات والاعتداءات، ولكن من زاوية تقنية ضيقة، وضمن هذه يمكن الاشارة الى خمسة انواع من الاساليب بعضها يتصل بالهجمات التي تستهدف نظام او استراتيجية الدخول، وبعضها يستهدف نظام ادخال ومعالجة البيانات، وبعضها يصنف كفعل اولي لتحقيق عمليات الدخول غير المصرح به الى مختلف انواع الشبكات، ونشير بايجاز الى هذه الاساليب والاعتداءات مع ايضاح لمسميات اخرى من الانشطة والاساليب والاعتداءات تتصل باختراق الشبكات تحديدا وبيان لاهم نقاط الضعف :

- العبث (الغش) بالبيانات Dat Diddling : ويستهدف هذا الهجوم او الاعتداء تغيير البيانات او انشاء بيانات وهمية في مراحل الادخال او الاستخراج، ويتم في الحقيقة بعشرات الانماط والاساليب التقنية.

- خداع بروتوكول الانترنت Ip Spoofing (التخفي باستغلال بروتوكولات النقل): ان اصطلاح Spoofing لا يعني التخفي، فهو اصطلاح يتعلق بالغش والخداع والايهام والتقليد والمحاكاة والسخرية، لكن استخدامه الشائع الان يتعلق بهجمات فايروسات الانترنت، اننا نتحدث هنا عن وسيلة تقنية بحته، بحيث يقوم المهاجم عبر هذه الوسيلة بتزوير العنوان المرفق مع حزمة البيانات المرسلة بحيث يظهر للنظام – على انه عنوان صحيح مرسل من داخل الشبكة، بحيث يسمح النظام لحزمة البيانات بالمرور باعتبارها حزمة مشروعة.
- جمع كلمات السر والتقلطها Password Sniffing: ان انشطة الاعتداء التي تتم باستعمال كلمات السر كانت تتم غالبا فيما سبق عن طريق تخمين كلمات السر مستفيدة من ضعف الكلمات عموما وشيوع اختيار الافراد لكلمات سهلة تتصل بمحيطهم الاسري او محيط العمل او حياتهم الشخصية، فان الجديد استخدام برمجيات يمكنه التقاط كلمات السر خلال تجوالها في جزء من الشبكة او احد عناصرها ومراقبتها ومتابعتها لحركة الاتصال على الشبكة، بحيث يقوم هذا البرنامج من حيث الاصل بجمع اول 128 بايت او اكثر – مثلا – من كل اتصال بالشبكة التي تجري مراقبتها وتتبع حركة الاتصال عليها، وعندما يطبع المستخدم كلمة السر او اسم المستخدم، فان البرنامج الجامع يجمع هذه المعلومات وينسخها اضافة الى ان انواع من هذه البرامج تجمع المعلومات الجزئية وتعيد تحليلها وربطها معا كما تقوم بعضها باخفاء انشطة الالتقاط بعد قيامها بمهمتها.
- المسح والنسخ:Scanning: وهو اسلوب يستخدم فيه برنامج (الماسح demon dialer processes) الذي هو برنامج احتمالات يقوم على فكرة تغيير التراكيب او تبديل احتمالات المعلومة، ويستخدم تحديدا بشان احتمالات كلمة السر او رقم هاتف المودم ، وابسط نمط فيه عندما تستخدم قائمة الاحتمالات

لتغيير رقم الهاتف بمسح قائمة ارقام كبيرة للوصول الى احداها الذي يستخدم موديم للاتصال بالانترنت، او اجراء مسح لاحتمالات عديدة لكلمة سر للوصول الى الكلمة الصحيحة التي تمكن المخترق من الدخول للنظام.

- هجومات استغلال المزايا الاضافية Excess Privileges : الفكرة هنا تتصل بواحد من اهم استراتيجيا الحماية، فاللاصل ان مستخدم النظام –تحديدا داخل المؤسسة – محدد له نطاق الاستخدام ونطاق الصلاحيات بالنسبة للنظام، لكن ما يحدث في الواقع العملي ان مزايا الاستخدام يجري زيادتها دون تقدير لمخاطر ذلك او دون علم من الشخص نفسه انه يحظى بمزايا تتجاوز اختصاصه ورغباته، في هذه الحالة ان اي مخترق للنظام لن يكون فقط قادرا على تدمير او التلاعب ببيانات المستخدم الذي دخل على النظام من خلال اشتراكه او عبر نقطة الدخول الخاصة به، انه ببساطة سيتمكن من تدمير مختلف ملفات النظام حتى غير المتصلة بالمداخل الذي دخل منه لانه استثمر المزايا الاضافية التي يتمتع بها المستخدم الذي تم الدخول عبر مدخله، وهذا وحده يعطينا التصور لاهمية استراتيجية امن المعلومات وحمايتها في المنشاء فان تحديد الامتيازات والصلاحيالت قد يمنع في حقيقته من حصول دمار شامل ويجعل الاختراقات غير ذي اثر، ولن تسمح الاستراتيجيات الواعية للقول ان المستخدم الفلاني لديه مزايا لا يعرف عنها بل لن تسمح بوجودها اصلا(20).

المحور الرابع: التحليل الاحصائي والاستنتاجات والتوصيات

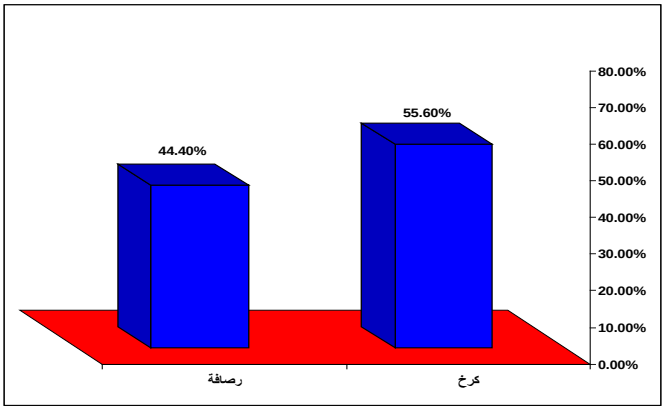
التحليل الاحصائي

صمم لاستبيان من أجل تقصي سلوك المستهلكين تجاه الخصوصية المعلوماتية ومخاطر التقنيات الحديثة عليها لتحقيق الأهداف المرجوة من البحث، وعرضت على عدد من المحكمين (د. منى تركي الموسوي، د. خليل إسماعيل إبراهيم، د عارف محسن، د. محمد عبد الرزاق الصوفي، د. اسعد خلف، د. عارف محسن) في كافة الاختصاصات التي لها علاقة مباشرة بالبحث (الاقتصادية والمالية والنفسية)، وتم الاخذ بتوجيهاتهم في نظر الاعتبار لكي تخرج الاستبانة بشكل علمي ورصين. وشملت الدراسة الميدانية 407مبحوثا وزعت الاستبانات عشوائيا على عينة من مواطني محافظة بغداد حيث استجاب للاستبيان 399 مواطن في حين لم يستجب ما تبقى من العينة لتلك الاستبانة.

تم استخدام البرنامج الاحصائي الجاهز SPSS في ادخال بيانات الاستبانات وتحليلها احصائيا وكانت نتائج التحليل مبينة كما ياتي:-

الجزء الأول: تضمن المعلومات الديموغرافية المتعلقة بالعينة المبحوثة.

- **القضاء:**- أظهر التحليل الاحصائي ان كثر من نصف العينة المستطلعة (55.6%)هم من سكنة قضاء الكرخ، في حين ما تبقى من افراد العينة(44.4%) من سكنة قضاء الرصافة وكما مبين في الشكل (1) والجدول (1) ادناه

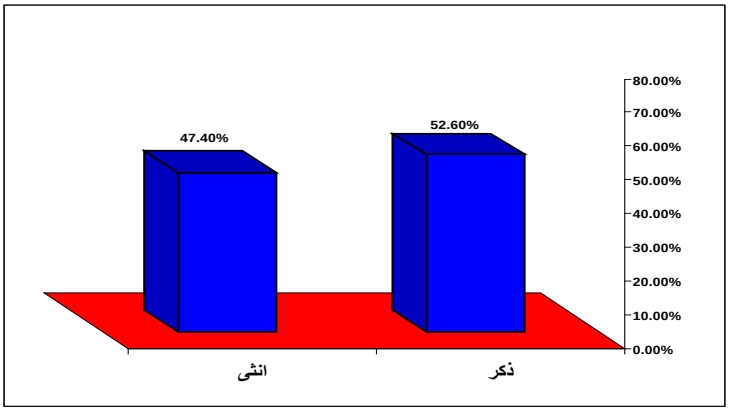


الشكل (1)

القضاء	التكرار	النسبة المئوية
كرخ	222	%55.6
رصافة	177	%44.4
المجموع	399	%100

جدول (1)

- **الجنس:**- أظهر التحليل الاحصائي أن ما يقارب(53%)من المستطلعين هم من الذكور، بينما كانت بقية العينة من الاناث وكما مبين ذلك في الشكل (2) و الجدول (2) ادناه.

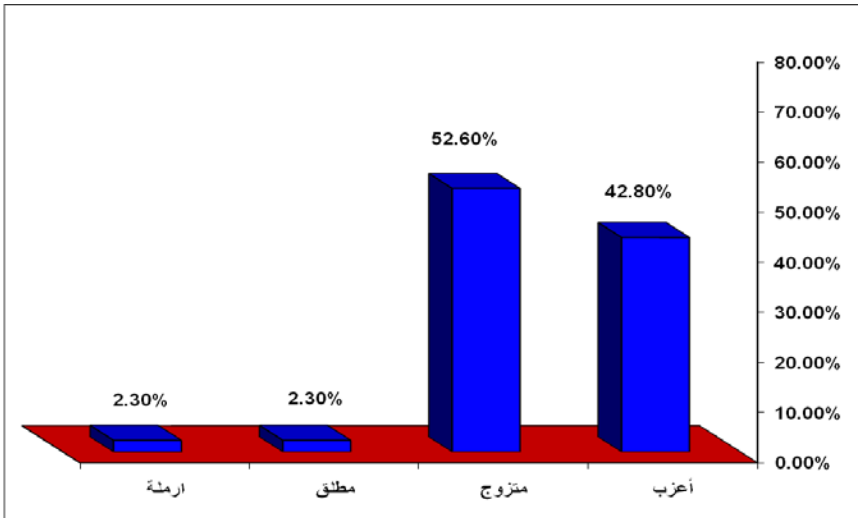


الشكل(2)

الجنس	التكرار	النسبة المئوية
ذكر	210	%52.6
انثى	189	%47.4
المجموع	399	%100

جدول (2)

- **الحالة الاجتماعية:**- يبين الشكل (3) والجدول (3) بان (42،9%) من المبحوثين كانوا عزابا، في حين كان أكثر من نصف العينة بقليل (52،6%) متزوجين، في حين تساوت نسبة المطلقين والارامل اذ بلغت(2،3%).

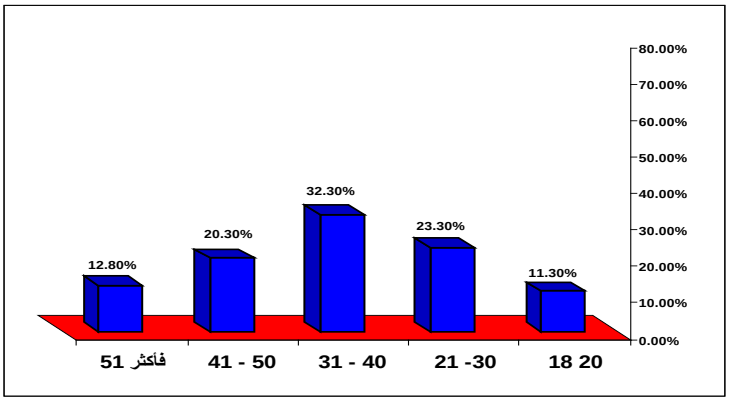


الشكل (3)

الحالة الاجتماعية	التكرار	النسبة المئوية
أعزب	171	%42.8
متزوج	210	%52.6
مطلق	9	%2.3
أرملة	9	%2.3
المجموع	399	%100

الجدول(3)

- **العمر**:- تصدرت الفئة العمرية (31-40) سنة أعمار المبحوثين اذ بلغت حوالي ثلث العينة المدروسة (32،3%) تلتها الفئة العمرية (21-30) سنة وبنسبة مئوية بلغت (23،3%)، وحلت الفئة العمرية (41-50) سنة ثالثا وبنسبة بلغت (20،3%)، وجاءت بعدها الفئة العمرية (51 – فأكثر) في المرتبة الرابعة وبنسبة بلغت (8،12%)، في حين ما تبقى من افراد عينة الدراسة (11,3%) فكانوا من الفئة العمرية(18-20) سنة الشكل (4) والجدول (4) يبينان النتائج.

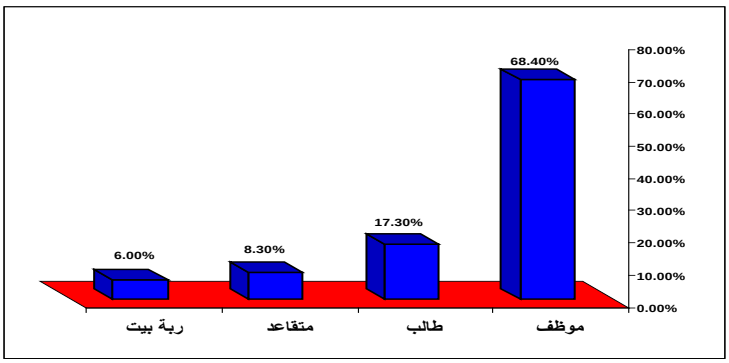


الشكل (4)

العمر	التكرار	النسبة المئوية
20 -18	45	%11.3
30 – 21	93	%23.3
40 – 31	129	%32.3
50- 41	81	%20.3
51 فأكثر	51	%12.8
المجموع	399	%100

الجدول (4)

- **المهنة:** – لوحظ زمن خلال التحليل الاحصائي بان أكثر من ثلثي العينة بقليل هم من الموظفين (68,4%)، تلاهم الطلبة وبنسبة مئوية قدرها (17,3%)، في حين كان ما تبقى من افراد العيتة من المتقلعدين وربات البيوت اذ كانت نسبهم المئوية (8,3%) و (6%) على التوالي و الشكل (5) والجدول (5) يوضحان النتائج أعلاه.

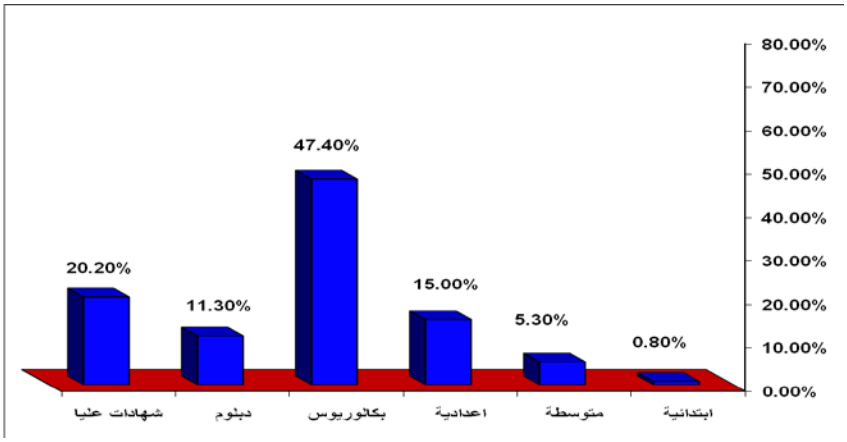


الشكل (5)

الوظيفة	التكرار	النسبة المئوية
موظف	273	%68.4
طالب	69	%17.3
متقاعد	33	%8.3
ربة بيت	24	%6.0
المجموع	399	%100

الجدول (5)

- **التحصيل العلمي:-** يبين الشكل (6) والجدول (6) بأن ما يقارب نصف العينة المدروسة هم من حملة شهادة البكالوريوس (47,4%)، تلاهم حملة الشهادات العليا وبنسبة بلغت (20,3%)، في حين جاء حملة الشهادة الاعدادية ثالثا وبنسبة مئوية بلغت (15%) اما حملت شهادة الدبلوم فشكلو حوالي (11,3%) من العينة، اما ما تبقى من المبحوثين فكانوا من حملتي الشهادتين المتوسطة والابتدائية وبنسب (5,3%) و (0,8%) على التوالي.



الشكل (6)

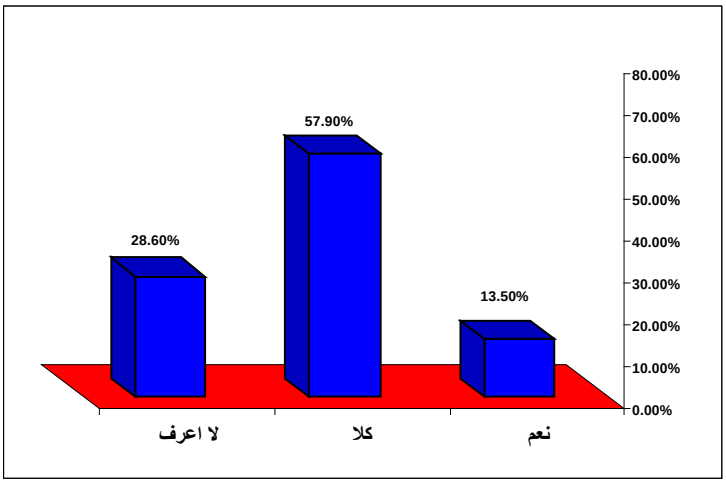
التحصيل العلمي	التكرار	النسبة المئوية
ابتدائية	3	%0.8
متوسطة	21	%5.3
اعدادية	60	%15.0
بكالوريوس	189	%47.4
دبلوم	45	%11.3
شهادات عليا	81	%20.2
المجموع	399	%100

الجدول (6)

والجزء الثاني : تضمن ثقل البحث من حيث التعرف على سلوك المستهلكين من المستطلعين تجاه الخصوصية المعلوماتية وعلى النحو الاتي:-

١ -**الخصوصي المعلوماتية وتطبيقها في العراق:-**

عند شؤال العينة المبحوتة فيما اذا كانوا يعتقدون بأن سياية حماية الخصوصية المعلوماتية فيما اذا كان يتم تطبيقها ومراعاتها في العراق، اشار اقل من ثلثي العينة المدروسة (57,9%) بعدم اقتناعهم بذلك، في حين وافقت نسبة من المستطلعين قدرها (13,5%) ذلك الامر واتفق معه، بينما لم يبدي ما تبقى من المستطلعين (28,6%) أي رأي حول هذه القضية، والشكل (7) والجدول (7) يبينان النتائج كما في ادناه.



الشكل (7)

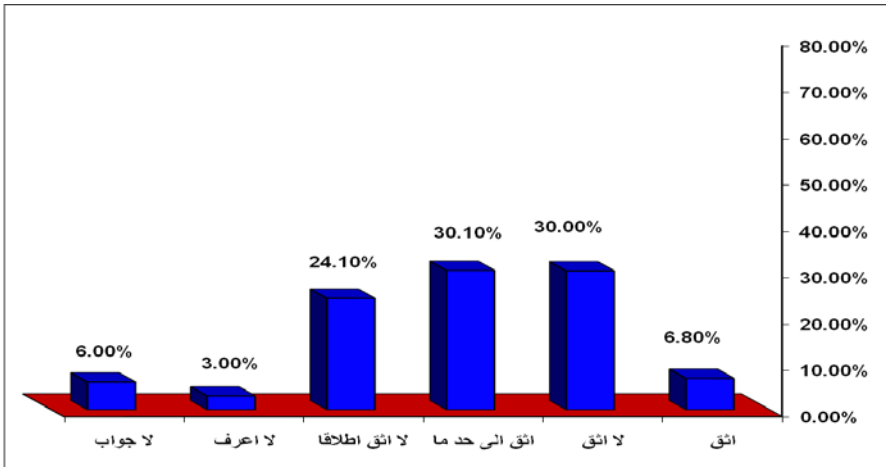
الحالة	التكرار	النسبة المئوية
نعم	54	%13.5
كلا	231	%57.9
لا اعرف	114	%28.6
المجموع	399	%100

الجدول (7)

٢ -**عينة الدراسة وثقتهم بمؤسسات الدولة:-**

لذا سؤال المستطلعين فيما اذا كانوا يثقون بالمؤسسات الحكومية التي يزودونها بمعلوماتهم الشخصية من عدمه، أظهرالشكل (8) والجدول (8) انقساما في ثقة المبحوثين اذ اشار ما يقارب (30,1%) منها بانهم يثقون الى حد ما، واشارت نفس النسبة من المبحوثين بعدم ثقتهم، وايدهم (24,1%) من المبحوثين بعدم ثقتهم المطلقة على خصوصيتهم المعلوماتية لدى المؤسسات الحكومية في الوقت الحاضر، في حين

كانت نسبة الذين لديهم ثقة تامة(6,8%)، بينما لم يجب ما تبقى من المستطلعين ولم يقرروا اجابة محددة حيث كانت نسبهم (6%) و(3%) على التوالي.



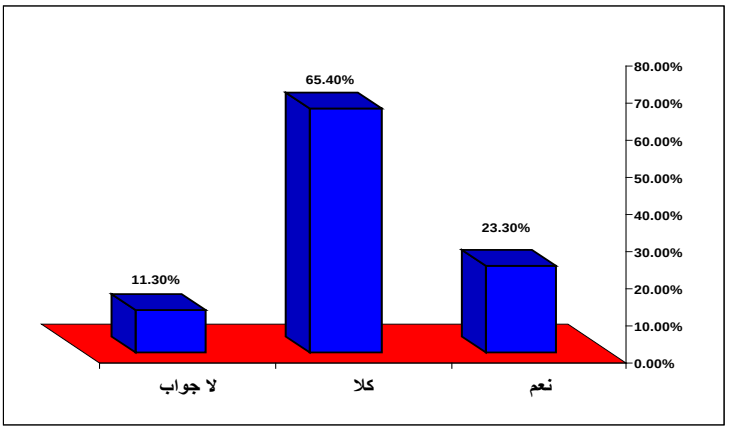
الشكل (8)

الحالة	التكرار	النسبة المئوية
اثق	27	%6.8
لا اثق	120	%30.0
اثق الى حد ما	120	%30.1
لا اثق اطلاقا	96	%24.1
لا اعرف	12	%3.0
لا جواب	24	%6.0
المجموع	399	%100

الجدول (8)

٣ -**الخصوصية المعلوماتية والبريد الالكتروني:-**

عند الاستفسار من عينة الدرسة حول امكانية وضعهم لوثائقهم الشخصية في بريدهم الالكتروني، رفض ما يقارب ثلثي العينة (65,4%) وضع مستمسكاتهم الشخصية ضمن بريدهم الالكتروني، في حين وضع (23,3%) من المستطلعين مستمسكاتهم في بريدهم الالكتروني، في حين لم يبدي ما تبقى في العينة (11,3%) اية اجابة تذكر والشكل (9) والجدول (9) يوضح ذلك.



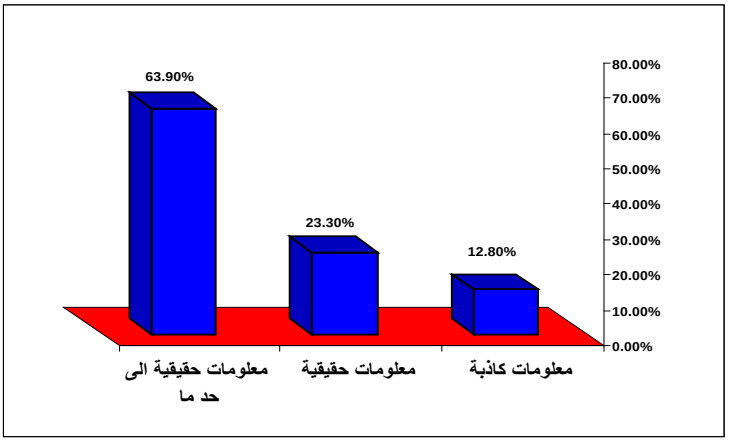
الشكل (9)

الحالة	التكرار	النسبة المئوية
نعم	93	%23.3
كلا	261	%65.4
لا جواب	45	%11.3
المجموع	399	%100

الجدول (9)

٤ -الخصوصية المعلوماتية ومواقع الانترنت:-

يبين الشكل (10) والجدول (10) بأن ما يقارب ثلثي عينة الدراسة (63,9%) يقدمون معلومات حقيقية الى حد ما عندما يشتركون في مواقع الشبكة العنكبوتية، في حين يقدم اقل من ربع عينة الدراسة (23,3%) معلومات حقيقية تامة، بينما كانت نسبة الذين يقدمون معلومات كأذبة عند اشتراكهم بمواقع الانترنت (12,8%).



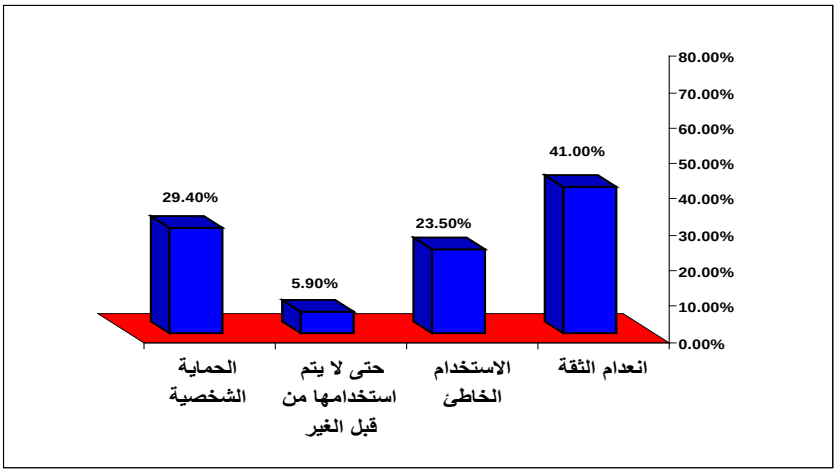
الشكل (10)

الحالة	التكرار	النسبة المئوية
معلومات كاذبة	51	%12.8
معلومات حقيقية	93	%23.3
معلومات حقيقية الى حد ما	255	%63.9
المجموع	399	%100

الجدول (10)

٤ -أ- اسباب تقديم المعلومات الكاذبة عند الاشتراك في مواقع الانترنت:-

لدى سؤال الذين يقدمون معلومات كاذبة عند اشتراكهم بمواقع الانترنت عن اسباب ذلك، اشار (41,2%) منهم بانهم لا يثقون بمواقع الانترنت تلك، في حين رأى (29,9%) منهم ان السبب هو تحفظهم على معلوماتهم الشخصية، وعلل حوالي ربعهم (23,5%) ذلك خوفا من الاستخدام الخطئ. فيما رأت نسبة ضئيلة جدا منهم 0,8% ان السبب وراء وضعهم المعلومات الكاذبة لكي لا يتم استخدامها من قبل الغير، والشكل (11) والجدول (11) يبين النتائج اعلاه.



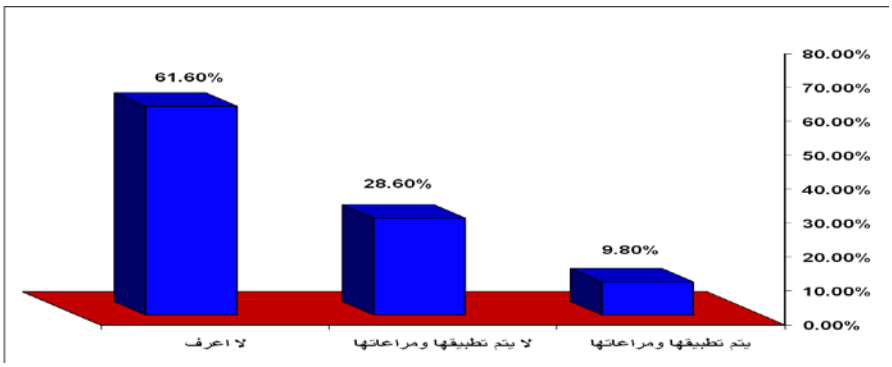
الشكل (11)

الحالة	التكرار	النسبة المئوية
انعدام الثقة	21	%41.2
الاستخدام الخاطئ	12	%23.5
حتى لا يتم استخدامها من قبل الغير	3	%5.9
الحماية الشخصية	15	%29.4
المجموع	51	%100

الجدول (11)

٥ -مصداقية مواقع الانترنت والخصوصية المعلوماتية:-

عند سؤال عينة الدراسة حول تصورهم فيما اذا كانت مواقع الانترنت تلتزم وتفي بساسة حماية معلوماتهم عند اشتراكهم بتلك المواقع، اشار (28,6%) من المستطلعين بعدم تطبيق مواقع الانترنت ومراعاتها لحماية خصوصيتهم المعلوماتية، في حين رأى (9,8%) منهم بان مواقع الانترنت تلتزم بذلك، ولم يبدي (61,7%) اي أجابة حول هذا السؤال والشكل (12) والجدول (12) يبين ذلك.



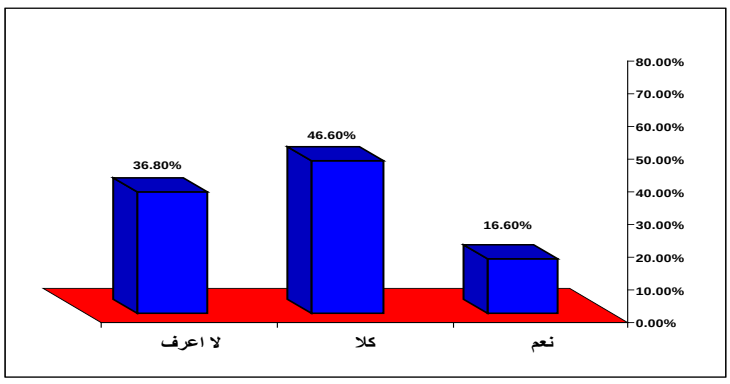
الشكل (12)

الحالة	التكرار	النسبة المئوية
يتم تطبيقها ومراعاتها	39	%9.8
لا يتم تطبيقها ومراعاتها	114	%28.6
لا اعرف	246	%61.6
المجموع	399	%100

الجدول (12)

٦ - العينة المستطلعة وانتهاكات خصوصياتهاالمعلوماتية:-

يبين الشكل (13) و الجدول (13) بان حوالي (46,6%) منهم لم يتعرضوا الى انتهاك او تجسس طال معلوماتهم، في حين اكد (16,5%) من المبحوثين بانهم قد تعرضوا الى انتهاك او تجسس طال خصوصياتهم المعلوماتية، في حين لم يعرف (36,8%) فيما اذا كانوا قد تعرضوا الى مثل هذا النوع من الانتهاك ام لا.



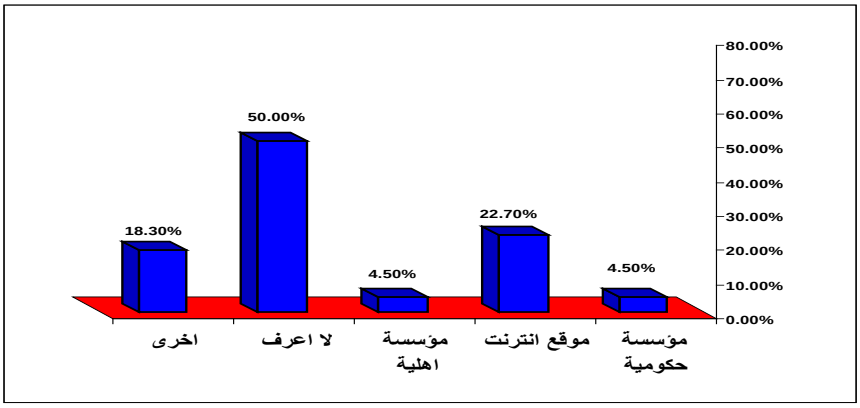
الشكل (13)

الحالة	التكرار	النسبة المئوية
نعم	66	%16.6
كلا	186	%46.6
لا اعرف	147	%36.8
المجموع	399	%100

الجدول(13)

٧ -**عينة الدراسة والجهات المنتهكة لمعلوماتهم الشخصية:-**

عند الاستفسار من المبحوثين الذين اكدوا بان معلوماتهم الشخصية قد انتهكت حول الجهات التي قامت بذلك العمل كانت اغلب الجهات المنتهكة مواقع الانترنت وبنسبة بلغت (22,7%)، تلتها الانتهاكات من قبل الافراد وبنسبة (18,2%)، في حين تعرض (4,5%) منهم الى انتهاكات من قبل مؤسسات حكومية، وساوتها نسبة الذين تعرضوا الى انتهاكات من قبل المؤسسات الاهلية، ولم يعرف نصف العينة تماما من هي الجهة التي انتهكت خصوصية معلوماتهم والشكل (14) والجدول (14) ادناه يبينان النتائج.



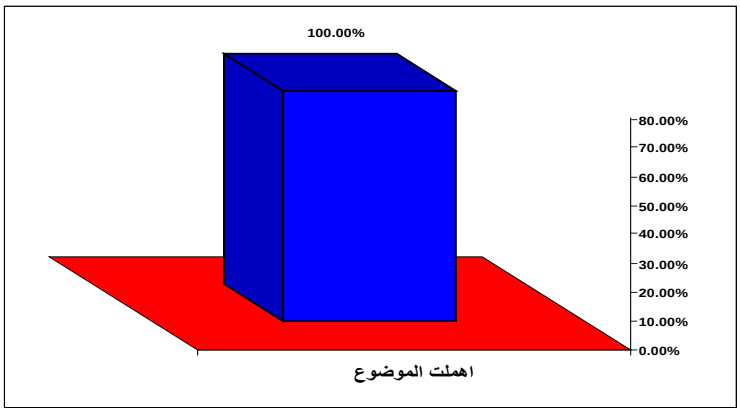
الشكل (14)

الحالة	التكرار	النسبة المئوية
مؤسسة حكومية	3	%4.5
موقع انترنت	15	%22.7
مؤسسة اهلية	3	%4.5
لا اعرف	33	%50.0
اخرى	12	%18.3
المجموع	66	%100

الجدول (14)

8- قرار المستطلعين تجاه الانتهاكات لخصوصيتهم المعلوماتية:-

عند الاستفسار من المبحوثين الذين انتهكت خصوصيتهم المعلوماتية عن القرار او الاجراء تجاه الجهات التي انتهكت معلوماتهم تلك، يظهر الشكل (15) والجدول (15) بان جميع المستطلعين الذين شملتهم الدراسة او الذين تعرضوا الى انتهاكات اهملوا الموضوع.



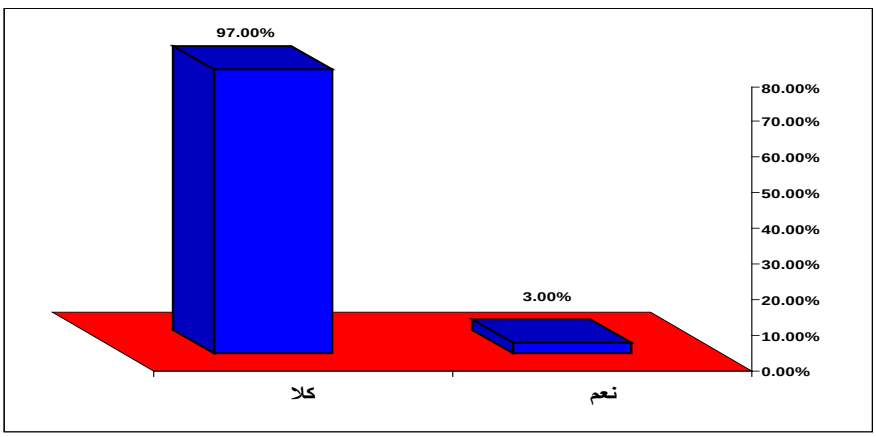
الشكل (15)

الحالة	التكرار	النسبة المئوية
اهملت الموضوع	66	%100.0
المجموع	66	%100

الجدول (15)

٩ -الخصوصية المعلوماتية والاشتراك في مواقع الانترنت والقانون العراقي:

تعتقد الاغلبية الساحقة من المستطلعين (97%) بعدم وجزد قوانين او تشريعات لحماية الخصوصية المعلوماتية في العراق من انتهاكات الجهات المختلفة، بينما تعتقد نسبة ضئيلة منهم هي (3%) بوجود قوانين او تشريعات عراقية حول هذا الموضوع والشكل (16) والجدول (16) يبين ذلك.



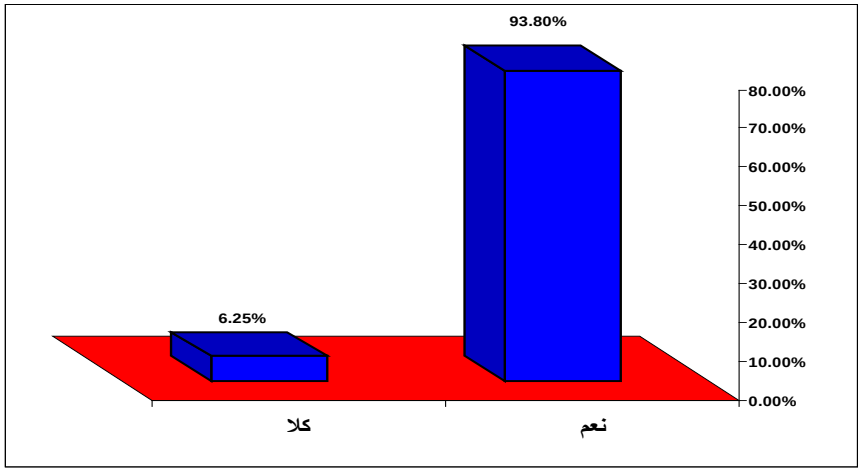
الشكل (16)

الحالة	التكرار	النسبة المئوية
نعم	12	%3.0
كلا	387	%97.0
المجموع	399	%100

الجدول (16)

١٠ – الخصوصية المعلوماتية والمشرع العراقي:

عند سؤال الاغلبية الساحقة من المبحوثين والتي تعتقد بعدم وجود قانون او تشريع عراقي يحمي المواطن وخصوصيته المعلوماتية من الانتهاكات المختلفة فيما اذا كانوا يطالبون المسؤلين بتشريع قوانين لحماية سرية المعلوماتية في العراق، طالبت الاغلبية الساحقة منهم بذلك وهي (93,8%)، في حين رأى ما تبقى من العينة (6,2%) عدم ضرورة ذلك، والشكل (17) والجدول (17) يوضح ذلك.



الشكل (17)

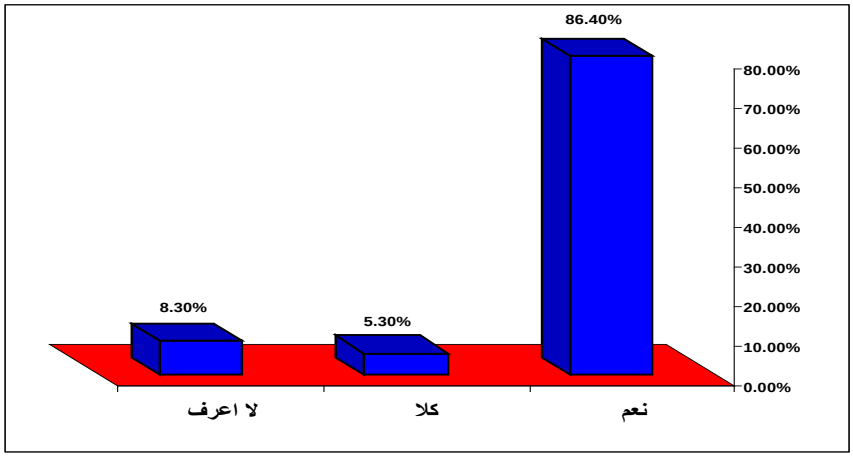
الحالة	التكرار	النسبة المئوية
نعم	363	%93.8
كلا	24	%6.2
المجموع	387	%100

الجدول (17)

١١ – التوعية والتثقيف حول الخصوصية المعلوماتية:

لدى سؤال عينة الدراسة حول ضرورة ان يتلقى المواطنون ومستخدموا الانترنت توعية مكثفة حول حماية حقوقهم في الاحتفاظ بمعلوماتهم الشخصية، رأت الاغلبية العظمى منهم (86,5%) ضرورة ذلك، بينما

رأى (5,3%) منهم عدم الحاجة الى ذلك، ولم يبدي ما تبقى من المستطلعين (8,3%) اي رأي حول هذا الموضوع والشكل (18) والجدول (18) يبين ذلك.



الشكل (18)

الحالة	التكرار	النسبة المئوية
نعم	345	%86.4
كلا	21	%5.3
لا اعرف	33	%8.3
المجموع	399	%100

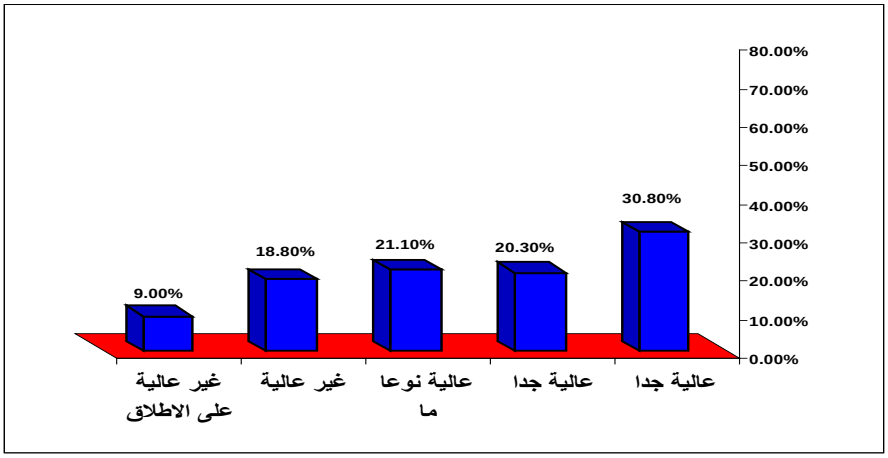
الجدول (18)

١٢ – درجة خطورة انتهاكات الخصوصية المعلوماتية:

لدى سؤال عينة الدراسة عن مدى خطورة او تصورهم لدرجة الاختراقات المبينة ادناه، كانت اجاباتهم على النحو الاتي:

أ – اتلاف وثائق الغير:

رأى أكثر من ثلاثة ارباع العينة المدروسة (72,2%) اتفاقهم وبدرجات مختلفة بان اتلاف وثائق الغير على درجة عالية من الخطورة، في حين ما تبقى من العينة (27,8%) يرون بان هذا الامر ليس بتلك الخطورة العالية والشكل (19) والجدول(19) يبين النتائج.



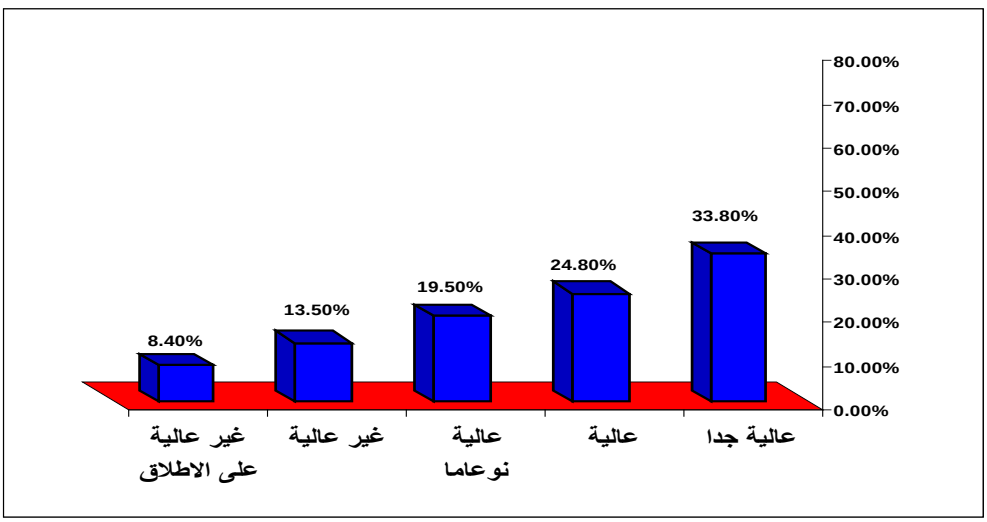
الشكل (19)

الحالة	التكرار	النسبة المئوية
عالية جدا	123	%30.8
عالية	81	%20.3
عالية نوعا ما	84	%21.1
غير عالية	75	%18.8
غير عالية على الاطلاق	36	%9.0
المجموع	399	%100

الجدول (19)

ب - تعريض اموال الناس للخطر:

يبين الشكل (20) والجدول (20) ان اكثر من ثلاثة ارباع العينة (78,2%) من المستطلعين يرون وبدرجات مختلفة خطورة تعريض اموال الناس للخطر، في حين ناقضهم الرأي (21,8%) ما تبقى من العينة حول ذلك الموضوع.



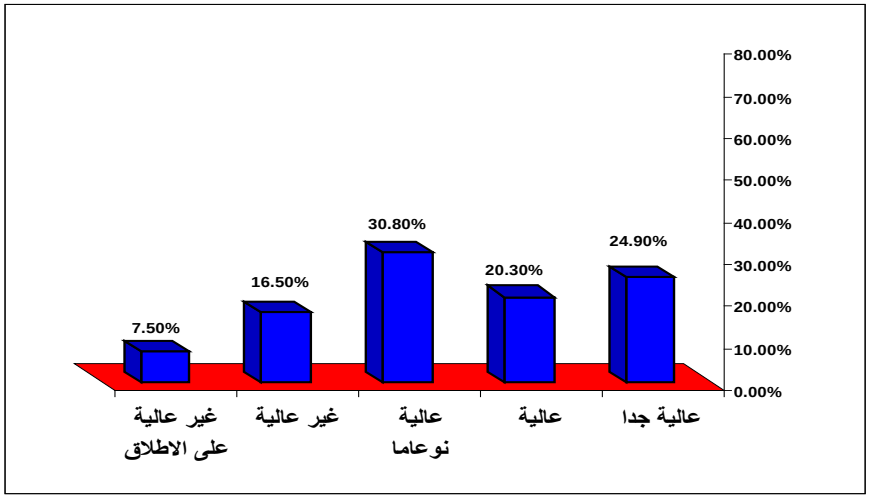
الشكل (20)

الحالة	التكرار	النسبة المئوية
عالية جدا	135	%33.8
عالية	99	%24.8
عالية نوعا ما	78	%19.5
غير عالية	54	%13.5
غير عالية على الاطلاق	33	%8.4
المجموع	399	%100

الجدول (20)

ج –أعتداء على وسائل الاتصال السلكية والغير سلكية:

يبين الشكل (21) و الجدول (21) بان اكثر من ثلاثة ارباع العينة بقليل (75,9%) يجمعون وبدرجات مختلفة على خطورة الاعتداء على وسائل الاتصال السلكية وغير السلكية، في حين لا يرون ما تبقى من العينة (42,1%) ذلك.



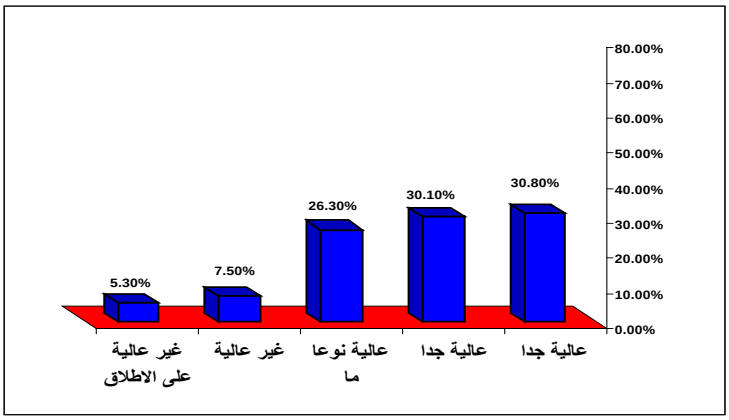
الشكل (21)

الحالة	التكرار	النسبة المئوية
عالية جدا	99	%24.9
عالية	81	%20.3
عالية نوعا ما	143	%30.8
غير عالية	66	%16.5
غير عالية على الاطلاق	30	%7.5
المجموع	399	%100

الجدول (21)

د- انتهاك حرية الغير:

يبين الشكل (22) والجدول (22) اتفاق عينة الدراسة وبدرجات مختلفة (87,2%) خطورة وجسامة حرية الغير، بينما يرى ما تبقى من العينة (12,8%) عدم خطورة ذلك الامر الى حد ما.



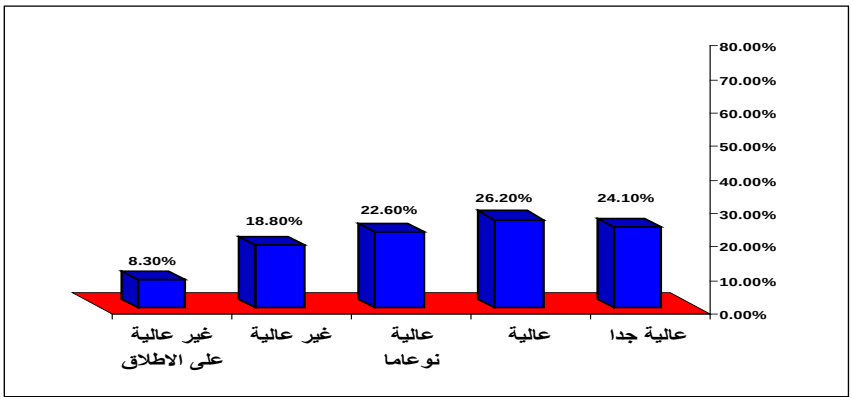
الشكل (22)

الحالة	التكرار	النسبة المئوية
عالية جدا	123	%30.8
عالية	120	%30.1
عالية نوعا ما	105	%26.3
غير عالية	30	%7.5
غير عالية على الاطلاق	21	%5.3
المجموع	399	%100

الجدول (22)

هـ- استخدام حساب البريد الالكتروني للغير:

يبين الشكل (23) و الجدول (23)، بان (72,9%) يرون بدرجات مختلفة خطورة استخدام حساب البريد الالكتروني للغير، بينما خالفهم الرأي (17,1%) من العينة المدروسة حول خطورة ذلك الامر.



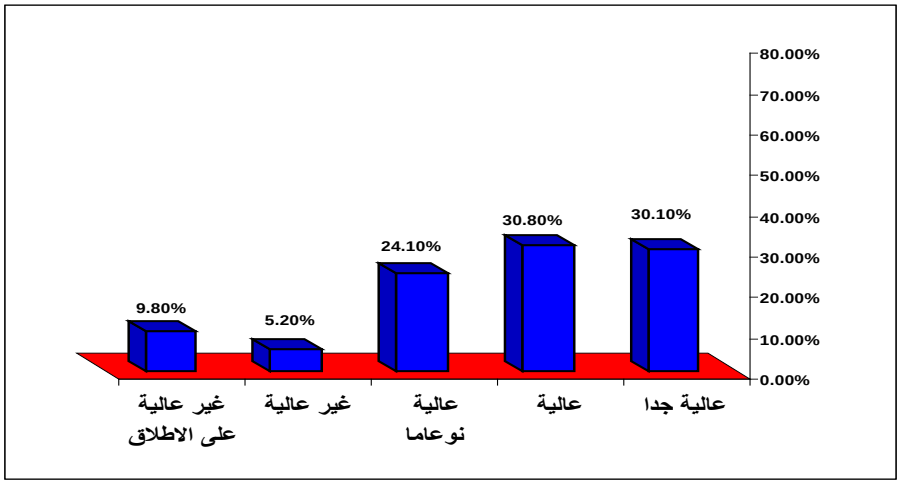
الشكل (23)

الحالة	التكرار	النسبة المئوية
عالية جدا	96	%24.1
عالية	105	%26.2
عالية نوعا ما	90	%22.6
غير عالية	75	%18.8
غير عالية على الاطلاق	33	%8.3
المجموع	399	%100

الجدول(23)

و- الحصول على كلمات العبور وأثارة مشاكل عبر البريد الالكتروني:

يبين الشكل (24) والجدول (24)، بان الاغلبية العظمى من المبحوثين (85%) يرون وبدرجات مختلفة خطورة سرقة كلمات العبور واثارت مشاكل فنية وامنية بالبريد الالكتروني للاخرين، بينما رأى ما تبقى (15%) منهم بان خطورة ذلك الامر غير عالية.



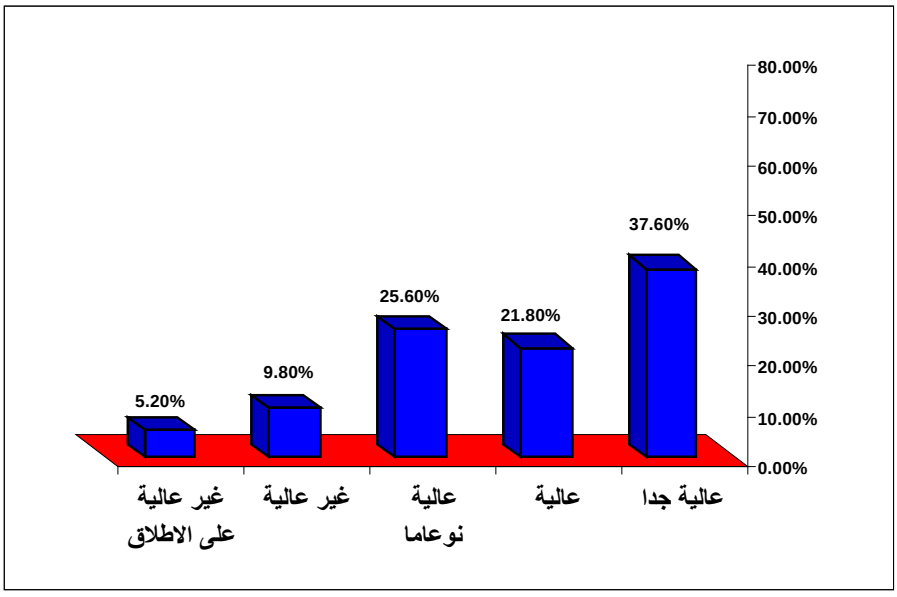
الشكل (24)

الحالة	التكرار	النسبة المئوية
عالية جدا	120	%30.1
عالية	123	%30.8
عالية نوعا ما	96	%24.1
غير عالية	21	%5.2
غير عالية على الاطلاق	39	%9.8
المجموع	399	%100

الجدول (24)

ز- استخدام البريد الالكتروني للاخرين في تناول وسائط تتنافى مع القيم والاخلاق:

يبين الشكل (25) والجدول (25) بان الاغلبية العظمى من المستطلعين (85%) يرون وبدرجات مختلفة خطورة استخدام البريد الالكتروني للغير في تناول وسائط تتنافى مع القيم والاخلاق، بينما خالفهما تبقى من العينة (15%) وبدرجات مختلفة ذلك الرأي.



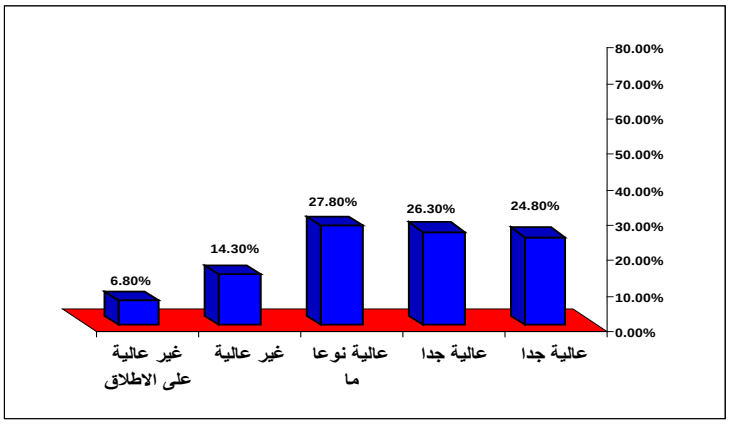
الشكل (25)

الحالة	التكرار	النسبة المئوية
عالية جدا	150	%37.6
عالية	87	%21.8
عالية نوعا ما	102	%25.6
غير عالية	39	%9.8
غير عالية على الاطلاق	21	%5.2
المجموع	399	%100

الجدول (25)

ح -استغلال موارد الشبكة لاغراض شخصية متعددة:

يبين الشكل (26) و الجدول (26) بان اكثر من ثلاثة ارباع العينة (78,9%) يرون وبدرجات مختلفة خطورة استغلال الشبكة العنكبوتية لاغراض شخصية متعددة، بينما خالفهم ما تبقى من العينة (21,1%) من المستطلعين الرأي وبدرجات مختلفة حول ذلك الامر.



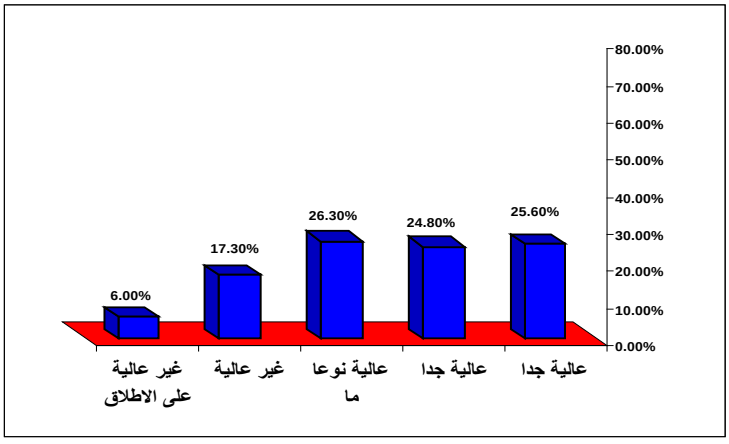
الشكل (26)

الحالة	التكرار	النسبة المئوية
عالية جدا	99	%24.8
عالية	105	%26.3
عالية نوعا ما	111	%27.8
غير عالية	57	%14.3
غير عالية على الاطلاق	27	%6.8
المجموع	399	%100

الجدول (26)

ط – اقتناص معلومات الشبكة الوطنية لاغراض شخصية بحتة:

يشير الشكل (27) و الجدول (27) الى ان اكثر من ثلاثة ارباع العينة بقليل (76,7%) يرون وبدرجات مختلفة خطورة التجسس على الشبكة الوطنية للمعلومات واقتناص المعلومات منها لاغراض شخصية بحتة، بينما يرى الباقون (23,3%) وبدرجات مختلفة عدم خطورة ذلك العمل.



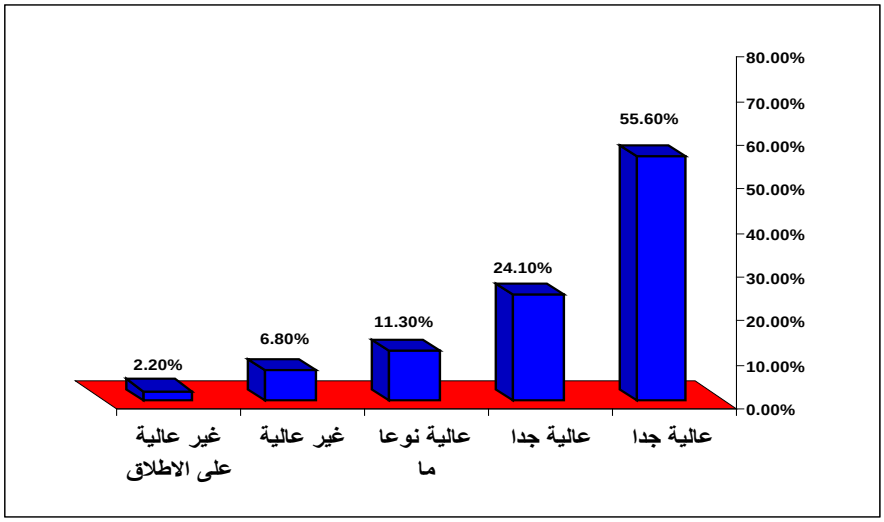
الشكل (27)

الحالة	التكرار	النسبة المئوية
عالية جدا	102	%25.6
عالية	99	%24.8
عالية نوعا ما	105	%26.3
غير عالية	69	%17.3
غير عالية على الاطلاق	24	%6.0
المجموع	399	%100

الجدول (27)

ي زج الفيروسات الحاسوبية لشبكة الانترنت وشبكة المعلومات الوطنية واحداث اضرار فيها:

يبين الشكل (28) والجدول (28) اجماع الاغلبية الساحقة من المستطلعين وبدرجات مختلفة وبنسبة (91%) خطورة وجسامة زج الفيروسات الحاسوبية لشبكة الانترنت وشبكة المعلومات الوطنية واحداث اضرار فيها، بينما رأت النسبة القليلة المتبقية (9%) عدم خطورة ذلك الامر.



الشكل (28)

الحالة	التكرار	النسبة المئوية
عالية جدا	222	%55.6
عالية	96	%24.1
عالية نوعا ما	45	%11.3
غير عالية	27	%6.8
غير عالية على الاطلاق	9	%2.2
المجموع	399	%100

الجدول (28)

- **الاستنتاجات والتوصيات:**

الاستنتاجات

إن رحلتنا في المسالك المتشعبة لشبكة الإنترنت الأخطبوطية، وتلمُّسنا للجوانب المعرفية التي أفرزتها هذه الشبكة، وطبيعة الانتهاكات القانونية التي يمكن أن تباشر من خلال فضائها الحاسوبي الكوني – الذي لم يَعُد يُعير اهتمامًا لمفاهيم الزمان والمكان التقليديين، وأرسى مفاهيمَ وأطرًا معرفية جديدة – تلفت انتباهنا إلى ضرورة مباشرة عملية معالجة قانونية محكمة لمسألة الانتهاكات السائدة في الفضاء الحاسوبي بشبكة الإنترنت، وباعتماد منطق قانوني تعالج من خلاله المحاور الاتية:

1- ان سياسة حماية الخصوصية المعلوماتية لا يتم تطبيقها في العراق في الوقت الراهن.

2- لا توجد ثقة كافية لدى المواطن المستطلع بدزائر ومؤسسات الدولة التي يزودونهمبمعلوماتهم الشخصية في الوقت الراهن.

3- لا توجد قوانين او تشريعات في العراق تحمي معلومات المواطن الشخصية من الانتهاك من قبل الاخرين.

4- تبرز ظاهرة اختراق الخصوصية المعلوماتية في مواقع الانترنت أكثر من هي عليه في المؤسسات الحكومية والمؤسسات الاهلية والاشخاص بشطل فردي.

5- ضرورة صياغة تعريف قانوني دقيق للفضاء الحاسوبي، تؤشر من خلاله الحدود التي يقيمها القانون لكل مفردة من مفرداته، على ضوء التقسيمات التي يفترضها ضمن مساحته الشاسعة، وشبكة العلاقات القائمة بين الجهات والأفراد التي تقيم في بقعته.

6 – ضرورة تقسيم الانتهاكات غير المشروعة السائدة في الفضاء الحاسوبي، بتوظيف أكثر من معيار قانوني، يعالج كلٌّ من هذه المعايير محورًا من محاورها، باعتبارها جريمة يحاسب عليها القانون (الخلف، 1982:297)، وكما ياتي:

المحور الأول: أنواع الجرائم من حيث جسامتها، وذلك بجعل معيار التمييز بين أنواعها على ضوء العقوبة التي قد حددت لكل منها.

المحور الثاني: أنواع الجرائم من حيث طبيعتها، فتُعالج من خلال هذا المحورِ طبيعةُ الحق المعتدَى عليه من قِبل الجرائم الحاسوبية، وتصنف على ضوء ذلك إلى جرائم سياسية تستهدف أمن الدولة الخارجي أو الداخلي،وعادية.

المحور الثالث: أنواع الجرائم من حيث أركانها الثلاثة: المادية، والشرعية، والمعنوية.

7- ضرورة معالجة موضوع انتهاك الحرمة الشخصية لملفات الغير وبياناتهم الشخصية، مهما كانت طبيعة المعلومات التي تتضمنها، وهذا الأمر يتطلب معالجةً قانونية دقيقة، تحدد من خلالها حدود الحرمة الشخصية لمواقع الأفراد على الشبكة، وماهية الصلاحيات القانونية المتاحة للغير في الدخول إليها عبر الوسائل المختلفة، وطبيعة الاستثناءات التي تخول بها بعض الجهات الرسمية لتفحص بعض محتوياتها، على ضوء طبيعة الظروف والملابسات التي تتطلبها.

8- إن دخول شبكة الإنترنت وتقانات المعلوماتية إلى كل شبر من ساحة الاستخدام اليومي للإنسان العربي المعاصر - باتت تحتم ضرورة التفكير في إعادة صياغة الكثير من فقرات الشرعية الدولية لحقوق الإنسان، التي لم تتوجه صوب المفاهيم الجديدة التي أرستها تقانات المعلوماتية بوقتنا الراهن.

9- حتمية إعادة صياغة قواعد قانونية جديدة لحماية الخصوصية المعلوماتية، وبما يتناسب مع التطور الحاصل في اختزان المعلومات، ونقلها، واستنساخها.

10- سينشب عن إتاحة الفرصة للجميع باستثمار القابليات المتاحة على الشبكة العنكبوتية، مع غياب سلطة المراقبة الأخلاقية في دول أخرى - أكثر من إمكانية لانزلاق زمرة من الشباب العربي، أو ضعاف النفوس في منحدرات الخطيئة، التي قد يستغلها البعض في إشاعة النزعات اللاأخلاقية؛ لذا يستلزم هذا الأمر معالجة حكيمة؛ لتجاوز هذه العقبة الأخلاقية التي تتعارض مع عاداتنا وأخلاقياتنا، من خلال مراقبة قانونية لموارد الشبكة.

التوصيات

1- ضرورة قيام المسؤلين بتشريع القوانين تحمي سرية الخصوصية المعلوماتية في العراق.

2- ضرورة تلقي مستخدمي الانترنت والمواطنين بشكل عام دورات تثقيفية حول حماية خصوصيتهم المعلوماتية.

3- اقامة الندوات والدورات والمؤتمرات حول هذا الموضوع من حيث مناقشة ابعاده وتاثيره على المجتمع العراقي.

المصادر

١. د. اسامة عبد الله قايد، " الحماية الجنائية للحياة الخاصة وبنوك المعلومات"، دار النهضة العربية، 1994

2. Roger Clarke, " personalia page", 2008

3. Westin, AF," Privacy and freedom, New York, Atheneum,1967

4. Miller, A," The assault on privacy, University of Michigan press,1971

5. Burkert, H," Institutions of data protection", 1982

6. Nugter,A.C.M,"Transborder flow of personal dat within the EC,Boston,1990

7. Michael, J, "Privacy and human Rights", An international and comparative study with special reference of development in information technology, 1994

8. Jerry Berman & Deirdre Mulligan, "Privacy in the digital age(the internet and law): work in progress", nova law review, volume 23, Number 2, 1999

9. See Joan E. Rigdon, " Internet users they'd rather not share their cookies", wall st.J, 1996

١٠. منشورات هيئة الامم المتحدة،" اعمال الامم المتحدة في ميدان حقوق الانسان"، المجلد الاول، نيويورك، 1990

١١. د. صالح جواد كاظم،" التكنولوجيا الحديثة والسرية الشخصية"، الطبعة الاولى،بغداد، 1991

١٢. د. هشام محمد فريد رستم،" قانون العقوبات ومخاطر تقنية المعلومات"، مكتبة الالات الحديثة، 1992

13. Dr. Malcolm O.Norris, Privacy and the legal aspects of the information superhighway, 2008

14. Ulrich sieber," Computer related crime", 1994

١٥. منير الجنبيهي،" جرائم الانترنت والحاسب الالي وطرق مكافحتها"، الطبعة الاولى، 2008

١٦. علي، نبيل،" الثقافة العربية وعصر المعلومات"، 2001

١٧. د. عمرو احمد جسبو،" حماية الحريات في مواجهة نظم المعلومات"، القاهرة، 2000

١٨. جمال محمد غيطاس،" أمن المعلومات والامن القومي"، دار نهضة مصر، 2007

١٩. د. موسى مسعود ارجوحة،" الارهاب والانترنت"، ابحاث المؤتمر الدولي لجامعة الحسين بن طلال، 2008

٢٠. منتدى الامن التقني والتكنولوجي،" حماية الخصوصية على الشبكات"، 2010

أستبانة معلومات

عزيزتي المواطنة ــ عزيزي المواطن

نهديكم اطيب التحيات

يقوم مركز بحوث السوق وحماية المستهلك في جامعة بغداد بأُجراء دراسة استطلاعية حول حماية الخصوصية المعلوماتية للمواطن العراقي. راجين تعاونكم معنا في ملئ الاستبانة بوضع علامة ( ) في المكان المناسب، خدمة للصالح العام. مع خالص الشكر والامتنان.

المعلومات الديموغرافية

- القضاء

كرخ ☐ رصافة ☐

- الجنس

ذكر ☐ أنثى ☐

- الحالة الاجتماعية

أعزب ☐ متزوج ☐ مطلق ☐ أرمل ☐

- العمر

20 – 18 ☐ 30 – 21 ☐ 40 – 31 ☐ 50 – 41 ☐ 51 فأكثر ☐

- المهنة

موظف ☐ طالب ☐ متقاعد ☐ ربة بيت ☐

- التحصيل العلمي

أمي ☐ ابتدائية ☐ متوسطة ☐ إعدادية ☐ بكالوريوس ☐ دبلوم ☐ شهادات عليا ☐

الخصوصية المعلوماتية

١. هل تعتقد أن سياسة حماية الخصوصية المعلوماتية يتم مراعاتها وتطبيقها في العراق؟

نعم ☐ كلا ☐ لا اعرف ☐

٢. هل تثق بجميع المؤسسات الحكومية التي تزودها بمعلوماتك الشخصية في الوقت الحاضر؟

نعم أثق ☐ لا اثق ☐ أثق الى حد ما ☐ لا اثق اطلاقا ☐ لا اعرف ☐ لا جواب ☐

٣. هل تضع في بريدك الالكتروني وثائقك الشخصية كالشهادة الجامعية، صور شخصية، هوية الاحوال المدنية..... وغيرها؟

نعم ☐ كلا ☐ لا جواب ☐

4 عندما تشترك باحد المواقع هل تقدم معلومات؟

معلومات كاذبة ☐ معلومات حقيقية ☐ معلومات حقيقية الى حد ما ☐

4.أ لماذا 1.....

2.....

3.....

5 . هل تعتقد أن مواقع الإنترنت ستلتزم حقيقة وتفي بسياسات حماية الخصوصية المعلوماتية لمعلوماتك التي ستزودهم بها ؟

يتم تطبيقها ومراعاتها ☐ لا يتم تطبيقها ومراعاتها ☐ لا أعرف ☐

٦. هل تعرضت في احد الايام الى انتهاك وتجسس على معلوماتك الشخصية؟

نعم كلا لا اعرف

٧. ما هي الجهة التي انتهكت معلوماتك الشخصية؟
مؤسسة حكومية موقع انترنت
مؤسسة اهلية أخرى تذكر .....

٨. هل قمت باتخاذ اجراء معين تجاه من انتهك معلوماتك الشخصية؟
نعم لجأت الى القضاء أهملت الموضوع

٩. هل تعتقد بان هناك قوانين في العراق تحمي معلوماتك الشخصية من انتهاك من قبل مواقع الانترنت
نعم كلا

أذهب الى فقرة 11

١٠. هل تطالب المسؤولين بتشريع قانون يحمي سرية المعلوماتية في العراق؟
نعم كلا

١١. هل من الضروري ان يتلقى مستخدموا الانترنت والمواطنون توعية مكثفة حول حماية حقوقهم في الاحتفاظ بمعلوماتهم الخاصة؟
نعم كلا لا أعرف

١٢. أن عملية الدخول الغير المشروع يمارسها الغير دون وجون حساب قانوني، وتعتبر اختراقا معلوماتيا يقع صاحبه تحت طائلة المسائلة القانونية؟ ما هي درجة تصورك للاختراقات على ضؤ المواضيع الاتية:

ت	الموضوع	درجة الاختراق		
		عالية	معتدلة	لا يوجد اختراق
1	اتلاف وثائق الغير			
2	تعريض اموال الناس للخطر			
3	الاعتداء على وسائل الاتصال السلكية واللاسلكية			
4	انتهاك حرمة الغير			
5	استخدام حساب البريد الالكتروني للغير			
6	الحصول على كلمات العبور(السر) واثارة مشاكل فنية او امنية ببريده الالكتروني			
7	استخدام البريد الالكتروني في تداول وسائط تتنافى مع الاخلاق والقيم			
8	استغلال موارد الشبكة لاغراض شخصية متعددة			
9	اقتناص معلومات من الشبكة الوطنية للمعلومات لاغراض شخصية بحتة			
10	زج الفيروسات الحاسوبية للشبكة واحداث اضرار فيها			

١٣. اية ملاحظات او مقترحات اخرى 1.....
2.....
3.....

نشكر تعاونكم معنا