Journal homepage:
http://ijimct.journals.ekb.eg/
Online ISSN: 2682-2881 Print ISSN: 2682-2105

Original Research Article

A Proposed Legislative System for Internet of Things in Kingdom of Saudi Arabia: A Prospective Study

Maryah alhossayin*
Teaching Assistant, Department of Information Science, College of Arts, King Saud University

Jabreel AL-Arishee[1].

Dean,Deanship of Development and Quality Chariman of Department and Professor of Information Sciences. King Saud University.Former member of SHoura Counsil of Kingdam of Saudi Arabia , Saudi Arabia.

ABSTRACT

This study presents a proposed system for organizing Internet of Things (IoT) in Saudi Arabia. First, an initial list of the proposed legislative system for IoT systems in Saudi Arabia is developed based on articles of laws, legislations, and guidelines of related existing systems of IoT applied in other countries. This study then uses content analysis approach to prepare a preliminary list of the basic aspects of IoT, and lastly Delphi technique is adopted as a basic approach to develop final list of the proposed legislative system for IoT systems in Saudi Arabia. This study identifies five aspects as major requirements for IoT systems. These aspects are ordered according to their importance from perspective of experts as following: Infrastructure, IoT Security, Transparency and IoT Data Quality, and Privacy. This study shows in both rounds of Delphi analysis the consensus of all phrases in all

Keywords:

Internet of Things, Legislative System, IoT Privacy, IoT Transparency, IoT Security, Data Quality, Infrastructure

[1] Corresponding author:Email: jeddah42@yahoo.com

aspects with ratio equal or greater than 80%. The study concludes with number of recommendations including the encouragement of future research to study separately each identified aspect from legal and informational side; and the importance of having implementing regulation or guidelines for the use of IoT and its services in the governmental, private, and third sectors.

Keywords:

إنترنت الأشياء، نظام تشريعي، خصوصية إنترنت الأشياء، شفافية إنترنت الأشياء، أمان إنترنت الأشياء، جودة البيانات، البنية التحتية

ABSTRACT

تهدف الدراسة إلى تقديم نظام مقترح لتنظيم إنترنت الأشياء في المملكة العربية السعودية؛ استنادًا إلى قوانين وتشريعات وضوابط دول أخرى من خلال استطلاع رؤى الخبراء فيما يتعلّق بإعداد هذا المقترح، والتعرف على الأنظمة المعمول بها في إنترنت الأشياء على مستوى العالم، والتعرف على مواد القوانين التي أُستخدمت في إعداد النظام التشريعي المقترح لأنظمة إنترنت الأشياء في المملكة العربية السعودية؛ واعتمدت الدراسة على المنهج الوصفي التحليلي من خلال مراجعة القوانين واللوائح والأنظمة، والضوابط التي وضعت لتنظيم إنترنت الأشياء في بعض دول العالم؛ من أجل إعداد قائمة بالجوانب الأساسية لإنترنت الأشياء. كما اتبعت المنهج الاستشرافي بأسلوب دلفاي كمنهج أساسي لهذه الدراسة؛ وتوصلت الدراسة إلى عددٍ من النتائج، أهمها: أن هناك خمسة متطلبات رئيسة لأنظمة إنترنت الأشياء، وهي مرتّبة حسب أهميتها من وجهة نظر الخبراء كالآتي (البنية التحتية– أمان إنترنت الأشياء– الشفافية وجودة بيانات إنترنت الأشياء– الخصوصية)؛ وبينت الدراسة وجود توافق في الرأي للعبارات التي شملتها كلتا الجولتين الأولى، والثانية والتي بلغت نسبتها لكل عبارات الجوانب الرئيسة فوق 80%؛ وخرجت الدراسة بمجموعة من التوصيات، أبرزها: تشجيع الباحثين بإجراء دراسات متعمقة بكل جانب من الجوانب التي تناولتها الدراسة، من الجانب القانوني المعلوماتي، وأهمية وجود لائحة تنفيذية أو ضوابط تتناسب واستخدام إنترنت الأشياء وخدماتها في القطاع الحكومي والخاص والقطاع الثالث.

مقدمة

وفّرت شبكة الإنترنت لعدّة سنوات مضت الوصول إلى المعلومات من خلال الحواسيب والهواتف الذكية. أما اليوم فقد أصبح الحصول على المعلومات عن طريق الأشياء من حولنا أمرًا سهلاً؛ مما خلق تطورًا جديدًا لمفهوم الإنترنت الذي أصبح يتحكم في جميع الأنشطة اليومية الرئيسة ومراقبتها بواسطة أجهزة قادرة على التقاط البيانات وإرسالها، وهو ما يعرف اليوم بإنترنت الأشياء(Internet of Things (IoT (Kopet, Hermann, 2011, 308).

ومع الاهتمام العالمي بالتحول الجذري إلى توظيف إنترنت الأشياء، فإن العديد من الدول، بما فيهم المملكة العربية السعودية، ترى أن إنترنت الأشياء بنيةً تحتيةً ذات أهمية عالية المستوى للنمو الاقتصادي؛ فقد وصل سوق إنترنت الأشياء في المملكة العربية السعودية إلى قرابة 4.5 مليار ريال عام 2018–2019، وقد كانت النسبة الأكبر من هذا السوق لأجهزة إنترنت الأشياء (المعدات Hardware) ثم الخدمات. ومن الملاحظ أن الإنفاق على خدمات إنترنت الأشياء في المملكة العربية السعودية ينمو بسرعة؛ مما سيجعلها أكبر سوق إنترنت الأشياء في التعاون الخليجي، وثالث أكبر سوق في الشرق الأوسط (Khalil, Jawad, 2019).

وقد أدّى النمو الهائل في عدد الأشياء المتصلة بالإنترنت في جميع أنحاء العالم إلى بدء إنترنت الأشياء في تحويل الصناعات والمجتمعات، وأصبح النقاش في الوقت الحالي يدور حول أهمية سنِّ قوانين تعمل على ضبط إنترنت الأشياء وخدماتها؛ حيث إن إنترنت الأشياء يؤثر على طريقة عمل جميع الأنظمة المرتبطة به، ويربط بين أنواع مختلفة من العمليات. وهذا الترابط يستند إلى البيانات. وقد قيل عند النقاش حول إنترنت الأشياء بأن "البيانات هي البنية التحتية"(Goodman, Ellen, 2015) . فإذا كانت البيانات هي البنية التحتية، فإن البيانات الضخمة التي تنتج من تقنيات إنترنت الأشياء ستؤثر على جميع أنواع

الأنشطة الاقتصادية والاجتماعية والمدنية؛ لذا ظهرت جهود عديدة من قبل بعض الدول، كالولايات المتحدة الأمريكية، والاتحاد الأوربي، والمملكة المتحدة في إرساء قوانين تحكم استخدام إنترنت الأشياء، وتحفظ البيانات التي يتم جمعها من خلاله.

مشكلة الدراسة

ينبغي النظر بالتأثير الذي تحدثه إنترنت الأشياء؛ كونها تقنية ناشئة وضرورة وضع ضوابط تنظيمية تحكمها وتقلّل من مخاطرها. ونظرًا لاهتمام حكومة المملكة العربية السعودية بتطبيق رؤية 2030؛ فوجود نظام يخصّ إنترنت الأشياء في المملكة له أهمّية كبرى؛ كونها ثورة تقنية تدخل جميع القطاعات وتؤثر على مستخدميها؛ فالنظام سيضمن حماية بيانات المستخدمين والشركات التي تعتمد أنظمة إنترنت الأشياء، وسيمكن الحكومة من وضع ضوابط تشجع اعتماد ونشر تقنية إنترنت الأشياء.

بعد تتبع الدراسات والبحوث العلمية في هذا الموضوع المهمّ الذي تناول سياسات وقوانين إنترنت الأشياء التي وضعتها بعض الدول، وكذلك التحديات التي تواجه مستخدميها سواءً على المستوى الفردي أو الوطني، وكذلك تتبّع مواد القوانين واللوائح والأنظمة والتشريعات وكذلك الضوابط التنظيمية التي جرى اعتمادها كقوانين تحكم إنترنت الأشياء في الدول الغربية والعربية، فقد وجد افتقارًا أو تناثرًا لمثل هذه القوانين في بعض الدول، وبعضها اعتمد على ضوابط وقوانين الإنترنت التي جرى وضعها سابقًا. ونظرًا لعدم وجود دراسات عربية وأجنبية (على حد علم الباحثة) تتعلق بقوانين وأنظمة إنترنت الأشياء في المملكة العربية السعودية؛ الأمر الذي شجّع الباحثة للقيام بالدراسة في هذا المجال؛ وذلك لاقتراح نظام تشريعي يقنّن خدمات إنترنت الأشياء في المملكة العربية السعودية في الجوانب الآتية: الخصوصية، والشفافية، والأمان، وجودة البيانات، والبنية التحتية.

تساؤلات الدراسة

سعت هذه الدراسة إلى وضع مقترحٍ تشريعيٍ لأنظمة إنترنت الأشياء في المملكة العربية السعودية من خلال الأسئلة الآتية:

- ما الأنظمة المعمول بها في إنترنت الأشياء على مستوى دول العالم؟
- ما المواد القوانين التي أُستخدمت في إعداد وبناء النظام التشريعي المقترح لأنظمة إنترنت الأشياء في المملكة العربية السعودية والمتمثلة في الأسئلة الآتية:
  - أ- ما مواد القوانين المتعلقة بجانب الخصوصية؟
  - ب- ما مواد القوانين المتعلقة بجانب الشفافية؟
  - ت- ما مواد القوانين المتعلقة بجانب الأمان؟
  - ث- ما مواد القوانين المتعلقة بجودة البيانات؟
  - ج- ما مواد القوانين المتعلقة بالبنية التحتية؟

أهداف الدراسة

هدفت هذه الدراسة إلى تقديم نظامٍ مقترح لتنظيم إنترنت الأشياء في المملكة العربية السعودية؛ استنادًا إلى قوانين وتشريعات وضوابط دول أخرى من خلال استطلاع رؤى الخبراء فيما يتعلّق بإعداد هذا المقترح. وعليه، فإن هذه الدراسة سعت لتحقيق الأهداف الآتية:

- التعرف على الأنظمة المعمول بها في إنترنت الأشياء على مستوى العالم.
- التعرف على مواد القوانين والضوابط والسياسات التي استخدمت في إعداد النظام التشريعي المقترح لأنظمة إنترنت الأشياء في المملكة العربية السعودية، والمتمثلة في الأهداف الآتية:
  - أ- التعرف على مواد القوانين المتعلقة بجانب الخصوصية.
  - ب- التعرف على مواد القوانين المتعلقة بجانب الشفافية.

ت- التعرف على مواد القوانين المتعلقة بجانب الأمان.

ث- التعرف على مواد القوانين المتعلقة بجودة البيانات.

ج- التعرف على القوانين المتعلقة بالبنية التحتية.

حدود الدراسة

اقتصرت الدراسة على الخبراء في المجال القانوني المعلوماتي في المملكة العربية السعودية، وهم أعضاء هيئة التدريس ممّن يحملون مؤهل: أستاذ مساعد، أستاذ مشارك، أستاذ في قسمي علم المعلومات وقسم القانون في جامعة الملك عبدالعزيز بجدة، وجامعة الملك سعود، والأميرة نورة بنت عبدالرحمن بالرياض والبالغ عددهم (30) خبيراً.

منهج الدراسة

اعتمدت الدراسة على منهج الوصفي التحليلي؛كما اعتمدت الدراسة على المنهج الاستشرافي باستخدام أسلوب دلفاي Delphi "الذي يعتمد في توقّعه للمستقبل على ما يتنبأ به مجموعة من الأشخاص المنشغلين بمجال موضوع الدراسة الذي يطلق عليهم مصطلح (الخبراء Experts)" .(Okoli, Chitu, Pawlowski, Suzanne, 2004). ويُعدُّ هذا المنهج هو الأنسب لموضوع الدراسة؛ حيث أُتبعت المنهجية الآتية في الدراسة:

- التعرّف على قوانين وضوابط ولوائح إنترنت الأشياء المستخدم على مستوى العالم.
- استعراض وشرح مواد القوانين واللوائح والسياسات والضوابط التي استخدمت في إعداد النظام التشريعي المقترح لأنظمة إنترنت الأشياء في المملكة العربية السعودية.
- اختيار مجموعة من الخبراء في المجال القانوني المعلوماتي بما يتوافق مع طبيعة الدراسة ومجالها.
- توجيه مجموعة من مواد القوانين؛ للوصول إلى اتفاقٍ في الآراء، وقد تم تكرار هذه المرحلة بغرض الوصول إلى مرحلة مرضية من الاتفاق.

- بناء مقترح لنظام تشريعي لأنظمة إنترنت الأشياء في المملكة العربية السعودية، والناتج عن الاتفاق الجماعي من قبل الخبراء المختصين.

الدراسات السابقة:

- دراسة وينستون ماكسويل وآخرون (2019) Winston Maxwell & others بعنوان "مقارنة بين جهود إنترنت الأشياء التنظيمية في الاتحاد الأوربي وأمريكا والصين" وهي عبارة عن نظرة شمولية للوائح التنظيمية المتعلقة بإنترنت الأشياء في بعض دول العالم؛ حيث اشتملت الدراسة على مقارنة تحليلية لجهود الاتحاد الأوروبي والولايات المتحدة الأمريكية والصين في وضع قيود تنظيمية لإنترنت الأشياء. وقد اتّبع الباحث أسلوب التحليل للمقارنة بين اللوائح.
- دراسة ألكساندرو توبوك و سيلفيا ماريا و غابرييل غاريس Alexandru Tabusca & Silvia-Maria & Gabriel Garais (2018) بعنوان: "إنترنت الأشياء وقانون الاتحاد الأوربي" التي هدفت إلى تقديم صورة عن الوضع الحالي لبيئة إنترنت الأشياء في الاتحاد الأوربي، خصوصًا فيما يتعلق بالمسائل القانونية التي ارتبطت بالاستخدام الهائل للأجهزة المتصلة بالإنترنت، وكيف أن الاستخدام البشري للتقنيات الحديثة يؤدي إلى ظهور متطلبات قانونية جديدة.
- دراسة سبيروس تزافستاس Spyros Tzafestas (2018) بعنوان "الأخلاق والقانون في عالم إنترنت الأشياء"التي بيّنت أن تشريعات إنترنت الأشياء لا تزال بحاجة إلى التطوير؛ حيث قدّم الباحث نظرة عامة عن دور الحكومات في إنترنت الأشياء ولوائح الاتحاد الأوربي والولايات المتحدة الأمريكية بشأن خصائص إنترنت الأشياء التي تنطوي على: أمن البيانات، والخصوصية، والشفافية، والثقة.

- دراسة مارك ووكر وآخرون Mark Walker & others (2018) بعنوان "الحكومات العالمية المنتظرة: دراسة دولية عن تنظيم إنترنت الأشياء" وقد قام هذا البحث بدراسة استقصائية نوعية للضوابط التنظيمية الناشئة التي تواجه أجهزة إنترنت الأشياء للمستهلكين في الاتحاد الأوروبي والولايات المتحدة. وقد قدّم الباحثون لمحة عامة عن الوضع التنظيمي الحالي، من خلال مسح ومقارنة نهج الضوابط التنظيمية الحالية في الاتحاد الأوروبي والولايات المتحدة.
- دراسة جوشي وآخرون Joshi & Others (2016) بعنوان "الاتجاهات الناشئة في معايير وتشريعات إنترنت الأشياء" التي أوضحت أن هناك حاجة إلى التركيز على جوانب تشريعات إنترنت الأشياء وبيّنت أنه لا يوجد تشريع محدد لأجهزة وبرامج إنترنت الأشياء في دولة الهند وأن المسودة المنقحة لضوابط إنترنت الأشياء الصادرة في أبريل 2015 من قبل حكومة الهند.
- دراسة مارتن سانت و أميناتا قاربا Martin Saint & Aminata Garba (2016) بعنوان "التقنية والسياسة الخاصة بإنترنت الأشياء في إفريقيا" التي ناقشت تقنية الأشياء والتطبيقات الخاصة بإنترنت الأشياء بالتركيز على جهود الدول الإفريقية. وقد هدفت إلى توفير أسس ومحاور للمناقشة من قبل الباحثين وواضعي سياسات إنترنت الأشياء. وقد استخدم الباحث أسلوب الدراسة الاستشرافية لدراسة القضايا المستقبلية في سياسة إنترنت الأشياء من منظور البلدان النامية؛ لتكون نقطة انطلاق لإنشاء سياسات إنترنت الأشياء في إفريقيا.

مفهوم إنترنت الأشياء

وصف العالم البريطاني (Kevin Ashton, 2009)، الذي أطلق مصطلح "إنترنت الأشياء" في عام 1999م، إنترنت الأشياء بأنها شبكة من "العينين والأذنين" لأجهزة الكمبيوتر.

وقد أكدت بعض المؤسسات أن إنترنت الأشياء يجب أن يركز بشكل أساسي على "الأشياء"، ولابد من البدء في تعزيز الذكاء في الأشياء؛ مما أظهر مفهومًا آخر بجانب إنترنت الأشياء، وهو ما يدعى بالجُسيم Spime، ويُطلق على أي كائن يمكن تتبعه عن بُعد؛ لاحتوائه على أجهزة استشعار مجهزة بإمكانية الاتصال اللاسلكي وذات إمكانيات متقدمة جعلت منه شيئًا ذكيًا(Atzori& others, 2010).

ويُعرف إنترنت الأشياء أيضًا بأنه "المستشعر الذي يقوم بوظيفة محددة، ويمكنه الاتصال بأجهزة أخرى"، وهو جزء من بنية تحتية تسمح بنقل وتخزين ومعالجة البيانات التي تم إنشاؤها من قبل المستخدمين أو الأنظمة الأخرى (Dorsemaine & others, 2015).

أما تحالف كاسا قراسا CASAGRAS الذي تم إعداده لتقديم دراسات لمساعدة المفوضية الأوربية والمجتمع العالمي في صياغة سياسة RFID، فقد عرف إنترنت الأشياء بأنه "عالم يمكن للأشياء فيه التواصل تلقائيًا مع أجهزة الحاسب وكذلك مع بعضها البعض لتقديم الخدمات للبشرية"؛ حيث عدَّ التحالف إنترنت الأشياء بنية تحتية عالمية تمكن من تقديم الخدمات عن طريق الربط بين الأشياء المادية والافتراضية اعتمادًا على تقنيات المعلومات والاتصالات الحالية والمتطورة(Atzori& others, 2010).

كما تعرف لجنة التجارة الفيدرالية (Federal Trade commission, 2015) إنترنت الأشياء بأنها أجهزة أو مستشعرات تربط وتنقل المعلومات فيما بينها عبر الإنترنت.

وتُعرف الباحثة إنترنت الأشياء بأنها شبكة تتيح لأشياء مادية إمكانية الرؤية والسمع والتفكير من خلال جعل الأشياء تتحدث فيما بينها، وتملك إحساسًا عن طريق تزويدها بأجهزة استشعار مناسبة، وكذلك قدرة على مشاركة المعلومات، واتخاذ القرارات، وتنفيذ المهام عن طريق الإنترنت؛ من أجل تحويل هذه الأشياء من تقليدية إلى أشياء ذكية لها قدرات معيّنة.

مخاطر إنترنت الأشياء

دخلت تقنية إنترنت الأشياء في مجالات مختلفة؛ نتيجة إمكانياتها في إدارة الأشياء، والتحكم بها عن بُعد؛ مما عكس أهميتها القصوى وضرورة التعامل معها. وعلى الرغم من ذلك، فإن هناك بعض المخاطر المتعلقة بها التي لا يمكن تجاهلها، ولكن يمكن تجازوها وحلّها. وقد صنّفت الباحثة هذه المخاطر على النحو الآتي:

قضايا الخصوصية المحتملة الناشئة من إنترنت الأشياء (IoT Privacy)

يُعدُّ إنترنت الأشياء أحد التقنيات المذهلة التي بدأت بالتأثير في حياتنا، وإمكانياتها لا حصر لها؛ فعلى سبيل المثال، يمكن أن توفر الأجهزة الصحية لإنترنت الأشياء الوصول إلى بيانات المريض الصحية؛ مما يؤدي إلى زيادة مراقبة الحالات الخطيرة والتفاعل المنتظم بين الطبيب والمريض. كما يمكن لأجهزة التشغيل الآلي في المنزل، كمنظمات درجة الحرارة الذكية، وأجهزة الإنذار، أن تتيح للمستخدمين التحكم في منازلهم عن بُعد. (Federal Trade Commission Staff Report, 2015)

لذا سيزداد عدد الأجهزة والأشياء المرتبطة ببعضها في المستقبل كجزء من إنترنت الأشياء، وهذا يرجع لزيادة التقنيات التي تمكن إنترنت الأشياء. وقد يتسبب إنترنت الأشياء في افشاء أو إتاحة بعض المعلومات الشخصية أو الحساسة؛ ولذا يزداد القلق بشأن مدى القدرة على المحافظة على الخصوصية(خليفة، 2012، 58). إذ إن إنترنت الأشياء يتم من خلاله جمع كمية هائلة من البيانات الشخصية ومعالجتها، وعند النظر إلى الخصوصية في إنترنت الأشياء، فقد ذكر (Weber, 2010) أنه عادة ما تكون هناك قضيتان رئيستان تدور حولها، وهما: رغبة الفرد بإخفاء أو الحفاظ على سرية معلوماته الشخصية؛ استخدام المعلومات بعد جمعها.

قضايا الشفافية (IoT Transparency)

تُعدُّ الشفافية أساسًا لتحقيق أقصى استفادة من بيانات إنترنت الأشياء، ولكن إذا لم يكن مزوّد خدمات إنترنت الأشياء شفّافًا حول كيفية استخدام البيانات التي تم جمعها، فإن هذا سيؤثر سلبًا على خصوصية المستخدم؛ لذا من المهم إعلام المستخدمين ليس فقط بالبيانات التي تم جمعها للحصول على معلوماتهم الشخصية، ولكن أيضًا بالمعلومات التي تم جمعها من طرق أخرى غير محددة(Weber, 2010, 123).

تسمح الشفافية للمستخدمين باطلاعهم على أداء إنترنت الأشياء وكذلك نتائج جمع بياناتهم، وتتضمن الشفافية خصائص عدّة، كالوضوح، والدقة، وسهولة الوصول، والصدق، وغيرها(Weber, 2010, 344).

القضايا الأمنية في إنترنت الأشياء (IoT Security)

يُعدُّ الأمن التحدي الرئيس لأي تطبيق متصل بالشبكة العالمية، وقد قُدِّمت دراسة استقصائية شاملة لقضايا الأمن في مستويات مختلفة من أنظمة إنترنت الأشياء، وأعطت نظرة عن أحدث المنشورات العلمية التي عالجت القضايا الأمنية في إنترنت الأشياء. ووفقًا للدراسة، فإن السرية والنزاهة والتوافر هي الشواغل الرئيسة لأمن بيانات إنترنت الأشياء(Mendez, Papapanagiotou, Yang, 2017,13)

توفير الأمن لأنظمة إنترنت الأشياء، هو أمر بالغ الأهمية لحماية البيانات الحساسة والبنى التحتية(Goyal & others, 2006,89)، وبدون مستوى جيد من الحماية، لا يصح للمستخدمين تبني أنظمة وتطبيقات إنترنت الأشياء.

جودة البيانات وإنترنت الأشياء (Data Quality)

تُعدُّ البيانات أحد الأصول القيمة في إنترنت الأشياء؛ لأنها تقدّم معلومات عن ظاهرة أو شخص أو كيان معين، فالبيانات التي يتم جمعها من الأشياء الذكية هي الأساس لاتخاذ قرارات ذكية وتقديم خدمات فعالة؛ فإذا كانت البيانات التي تم جمعها ذات جودة رديئة وغير دقيقة، فمن المحتمل أن تكون القرارات التي سيتم اتخاذها قرارات غير صحيحة وذات نتائج عكسية؛ فجودة البيانات تُعدُّ أمرًا ضروريًا لاكتساب مشاركة المستخدم وقبوله لخدمات إنترنت الأشياء المقدّمة (Goyal & others, 2006, 81).

البنية التحتية التقنية (Infrastructure)

عند تمديد إنترنت الأشياء، فإن العامل الأكثر أهمية هو تطبيق معيار متكامل للبنية التحتية المختلفة لإنترنت الأشياء؛ لذا لابد من إنشاء إمكانية التشغيل المتداخل بين الكائنات المختلفة، وتنظيم الشبكة بطريقة تجعل من السهل على الأجهزة التواصل فيما بينها وتحديد مسارها. إذ ترسل الملايين من أجهزة إنترنت الأشياء بياناتها –التي عادةً لا تتشابه فيما بينها– إلى أنظمة مركزية، فمثلاً بعض الأجهزة قد تجمع بيانات متعلقة بالرطوبة ودرجة الحرارة، في حين أن الأجهزة الأخرى قد تجمع البيانات المتعلقة بمواقع الأشخاص أو أنشطتهم اليومية. وفي النهاية يتم إرسال البيانات إلى خوادم السُحب أو إلى تطبيقات إنترنت الأشياء؛ ليتم تحليلها.(Gazis, 2017) لذلك وجود اتصالٌ موثوق وذو سرعة عالية له دورٌ كبير في تسهيل التواصل بين أجهزة إنترنت الأشياء.

استخدامات تقنيات إنترنت الأشياء في المملكة العربية السعودية

سوق تقنيات إنترنت الأشياء يسير باتجاه تصاعدي بحسب ما ذكرته شركة البيانات الدولية (IDC, 2019)، وأوضحت بأنه من المتوقع أن ينمو بمعدّلٍ سنويٍ مركّبٍ نسبته 19.5% خلال الفترة 2018–2023م، وهذا سيجعلها أكبر سوقٍ لإنترنت الأشياء في دول مجلس التعاون الخليجي.

والمؤسسات العامة والخاصة السعودية قد بدأت بتبني حلول تقنيات إنترنت الأشياء وغيرها من التقنيات المبتكرة؛ تحقيقًا لرؤية المملكة 2030، ويمكن ذكر بعضها كالآتي:

المدينة الذكية

بدأت المملكة العربية السعودية في منح عقود لبناء مدينة ذكية تبلغ تكلفتها 500 مليار دولار. وتبلغ مساحة هذه المدينة الذكية 10.230 ميلاً مربعًا. ومن المخطط أن تبلغ مساحة المدينة الذكية الجديدة 33 مرة مساحة أرض مدينة نيويورك الأمريكية. تُعدُّ المدينة الجديدة، التي تسمى نيوم، وتقع في الركن الشمالي الغربي للمملكة العربية السعودية، جزءًا رئيسًا من طموحات المملكة للتنويع، وذلك بعيدًا عن الاعتماد على عائدات النفط (Stone & others, 2018).

الرعاية الصحية

يشهد قطاع الرعاية الصحية في المملكة العربية السعودية طفرة في نشر التقنية المبتكرة؛ حيث أنفقت المملكة أكثر من 40 مليار دولا في عام 2018م؛ من أجل تمكين إنترنت الأشياء. ويُعد أكبر قطاع للرعاية الصحية في الشرق الأوسط؛ حيث تقوم وزارة الصحة بربط السجلات الصحية إلكترونيًا لأتمتة سير العمل وتحليل البيانات التي تم جمعها من المستشفيات وأجهزة التتبع الصحية. كما تعمل وزارة الصحة على شراكة مع بائعي التقنية الرائدين لتطبيق نظام إدارة رعاية المرضى الذي يتميز بمراقبة المرضى، ويهدف إلى تقليل

الحاجة إلى زيارة الأطباء. كما يتم استخدام إنترنت الأشياء من قبل المؤسسات الصحية العامة والخاصة لتحسين إدارة المخزون؛ حيث تتيح الخزائن الذكية الجرد الذاتي للأدوية (Khalil, Jawad, 2019,12).

التصنيع

لتنويع الاقتصاد، تمكن حكومة المملكة العربية السعودية بشكل استباقي من نمو التصنيع المحلي من خلال المنح والمبادرات الإستراتيجية الأخرى؛ إذ تحرص مؤسسات التصنيع الكبيرة في المملكة على استخدام البيانات التي تم إنشاؤها بواسطة المعدات لإجراء الصيانة التنبؤية والوقائية، وبالتالي تقليل التكاليف وخطر تعطل المعدات ووقتها (Khalil, Jawad, 2019,13).

التجزئة

نظرًا لاكتساب قطاع الترفيه والتجزئة أهمية كبرى في المملكة العربية السعودية في ظل رؤية 2030 وبرنامج التحول الوطني؛ فقد بدأت تجارة البيع بالتجزئة في الاستفادة من التقنية لتلبية الاحتياجات التجارية المتزايدة. ويستخدم تجار التجزئة وقطاع الترفيه بيانات سلوك المستخدمين وهوياتهم الرقمية لمعرفة رغباتهم المستقبلية. كما تمكن إدارة المخزون، التي تدعم من قبل إنترنت الأشياء، مراكز التسوق من دفع الكفاءات التشغيلية والتأثير على سلوك الشراء من خلال جعل الإعلانات أكثر ملاءمة واستهدافًا وجاذبية للمتسوقين (Khalil, Jawad, 2019,13).

الحاجة إلى نظام تشريعي لإنترنت الأشياء

يواجه المنظمون اليوم التأثير الذي قد يخلفه انتشار إنترنت الأشياء؛ كونه يصل عددًا كبيرًا من الأجهزة والأشياء ببعضها البعض، ولأجل تطوير إنترنت الأشياء وتشجيع الابتكارات التي يعدها لمجتمعاتنا، فإنه يتعين على هيئات صنع القرار السياسي والاقتصادي وضع لوائح مناسبة قادرة على التحكم بإنترنت الأشياء، وعليه، فالحاجة لوضع نظام تشريعي يحكم إنترنت الأشياء في المملكة العربية السعودية، يتمثل في الآتي:

1. انتشر استخدام تقنيات إنترنت الأشياء على المستوى الشخصي، وكذلك على مستوى معظم القطاعات الحكومية، فعلى سبيل المثال، يرتدي بعض الأشخاص الساعة الذكية معظم الوقت، والتي من شأنها جمع كمية هائلة من المعلومات الشخصية وكذلك السلوكية، ويحق للمستخدم أن يكون لديه معرفة مسبقة بنوع المعلومات الحساسة التي يتم جمعها (Cheng & others, 2012,579)
2. هناك قيمة مالية لبيانات مستخدمي إنترنت الأشياء، وتساعد بشكل كبير الشركات المصنّعة لتقنيات إنترنت الأشياء على بيع المزيد من المنتجات من خلال جمع بيانات المستخدمين دون علمهم لمعرفة سلوكياتهم. ولمنع ذلك؛ يجب إصدار نظام مناسب.(Siboni & others, 2016, 125)
3. تطبيق اللوائح والأنظمة على أجهزة إنترنت الأشياء تساعد على حماية أمن المستخدمين والحكومات والمؤسسات.
4. تقدّم تطبيقات إنترنت الأشياء فوائد اقتصادية واجتماعية، بما في ذلك الخدمات عن بُعد، ودعم اتخاذ القرارات، وتوظيف الموارد بشكل أفضل، والتحكم بالخدمات عن بُعد. وعلى الرغم من ذلك، تنشأ عدد من العوامل التي قد تؤثر على مصداقية تلك التطبيقات، والتي من شأنها أيضًا أن تؤثر على الخصوصية والأمن، وعدم تناسق المعلومات وقلة جودتها، وشفافية الإجراءات(PINTÓ, 2015, 3).

5. وضع نظام تشريعي لإنترنت الأشياء يعني تقليل المخاطر المرتبطة به، ويساعد في توفير معلومات واضحة وموجزة ودقيقة يمكن الوصول إليها، كما يعزّز الاندماج الرقمي والاتصال مع التقنيات الأخرى، كتقنية البلوك تشين، والطابعة ثلاثية الأبعاد، وغيرها من التقنيات(PINTÓ, 2015, 3).
6. نظام إنترنت الأشياء معقَّد؛ حيث يمكّن من ربط الأجهزة من مختلف الشركات المصنّعة أو مطوري البرامج، وهذا قد يؤدي لصعوبة في تحديد المسؤولية عندما تتعرض أطراف أو أنظمة للاختراق أو لأضرار عن منتجات يُساء استخدامها أو نتيجة لحوادث الأمان الرقمية غير المتوقعة، فوضع اللوائح والأنظمة يحدد المسؤوليات والإجراءات التي يجب اتخاذها جراء ذلك، والتي تهدف إلى ضمان حماية كلٍّ من المستخدمين والشركات التي تعتمد تطبيقات إنترنت الأشياء (PINTÓ, 2015, 3).

قوانين وأنظمة وسياسات إنترنت الأشياء

تُعدُّ إنترنت الأشياء تقنية حديثة وسريعة الإنتشار، ولحداثتها فقد أقرّت بعض الدول قوانين وضوابط لتنظيمها، وسعت لتطبيقها حماية للمستخدمين،وفيما يلي عرضاً لهذه الدول.

أولاً: الولايات المتحدة الأمريكية

تُعدُّ مصادر لوائح الخصوصية "قطاعية" بطبيعتها في الولايات المتحدة؛ إذ لا يوجد قانون خصوصية شامل يتناول حماية البيانات (Johnson, 2016, 79). ولدى بعض الولايات تشريعات وأنظمة تختص بها فيما يخص إنترنت الأشياء، كولاية كاليفورنيا وقانونها رقم SB 327 الذي يتطلب من جميع الأجهزة المتصلة بالإنترنت– مثل أجهزة التلفاز والهواتف والألعاب والأجهزة المنزلية– أن يكون لديها " ميزات أمان معقولة"(*).

(*) Information privacy: connected devices, SB-327. Retrieved from: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327

كما قامت مدينة نيويورك بنشر ضوابط Guidelines [(**2)] تتعلق باستخدام إنترنت الأشياء في المدينة، وقد اشتملت هذه القواعد على الآتي:

- الخصوصية والشفافية.
- إدارة البيانات.
- الأمان.
- البنية التحتية.

وقد أقرت مدينة نيويورك لائحة تنفيذية لقانون البيانات المفتوحة[(ǂ3)] برقم 2012/ 01 الذي يتعلق بنشر البيانات المفتوحة التي يمكن نقلها ومعالجتها رقميًا، كبيانات خدمات إنترنت الأشياء في مدينة نيويورك الذي أُقر عام 2012م. كما أصدرت المدينة سياسات تتعلق بالبيانات، ومن ضمنها بيانات إنترنت الأشياء، كسياسة تشفير البيانات[(&4)] التي تهدف لتصنيف البيانات واستخدام تقنية تشفير لكل بيان ونقلها وتخزينها بعد تشفيرها. أما سياسة تصنيف البيانات [(¥5)] فتهدف لتصنيف البيانات –ومن ضمنها بيانات إنترنت الأشياء– و تطبيق درجة الحماية المناسبة بناءً على تقييمها.

ثانياً: الاتحاد الأوربي

تتطلب خصوصية الاتصالات الإلكترونية حماية خاصة، ولم يتم التطرق لها في اللائحة العامة لحماية البيانات General Data Protection Regulation (GDPR) الذي يحمي خصوصية بيانات جميع مواطني الاتحاد الأوربي، وإعادة تشكيل الطريقة التي

(**) New York guidelines for Internet of Things. Retrieved from: https://iot.cityofnewyork.us/
(ǂ) ***Open Data Law***. Retrieved from: https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=649911&GUID=E650813B-B1E9-4E56-81BA-58261487DA4A
(&) ***Data Classification Policy***. Retrieved from: https://www1.nyc.gov/assets/doitt/downloads/pdf/encryption.pdf
(¥)***Encryption Policy***. Retrieved from: https://www1.nyc.gov/assets/doitt/downloads/pdf/data_classification.pdf

تتبعها المنظمات في المنطقة، والمتعلقة بخصوصية البيانات ,2016/114 (DIRECTIVE (EU) 2016).

لذا ركزت لائحة الخصوصية الإلكترونية e–Privacy Regulation، على حماية الخصوصية عندما يتم توصيل وتبادل البيانات إلكترونيًا. كما أن اللائحة تتعامل مع مواضيع محدّدة، وتعمل أحكام اللائحة العامة لحماية البيانات فوق لائحة الخصوصية الإلكترونية، وستواصل تطبيقها على المجالات الأوسع نطاقًا التي لا تغطيها لائحة الخصوصية الإلكترونية (European Data Protection Board, 2019, 3).

كما قدمت فرقة العمل العاملة بموجب المادة 29 ARTICLE 29 DATA PROTECTION WORKING PARTY لائحة تنفيذية مرتبطة بشفافية معالجة البيانات الشخصية الواردة في اللائحة العامة لحماية البيانات، والتي تنطبق على إنترنت الأشياء. وقد فسرت اللائحة ما جاء في المادة (12) –على وجه الخصوص– من اللائحة العامة لحماية البيانات. وتحدد المادة (12) القواعد العامة التي تنطبق على توفير المعلومات للمستخدمين (بموجب المادة 13–14)؛ البيانات المتعلقة بحقوق المستخدمين واتصالاتهم (بموجب المواد 15–22)؛ وانتهاكات البيانات (بموجب المادة 34) (ARTICLE 29 DATA PROTECTION WORKING PARTY, 2016, 6).

ثالثاً: المملكة المتحدة

نشرت وزارة الرقمية والثقافة والإعلام والرياضة في المملكة المتحدة the UK's Department for Digital، Culture Media and Sport (DCMS)، النسخة النهائية من وثيقة بعنوان Consumer Internet of Things (IoT) Security for manufacturers تحتوي على ضوابط تختص بأمن مستهلكي إنترنت الأشياء في 14 أكتوبر عام 2018. الهدف من هذه الوثيقة هو توفير قواعد لتحسين أمن منتجات إنترنت

الأشياء والخدمات المرتبطة بها. وسيسهم تنفيذ الضوابط الثلاثة عشرة في حماية خصوصية المستخدم وسلامته، وسيخفف من تهديد الهجمات التي تتم على أجهزة وخدمات إنترنت الأشياء غير الآمنة (The UK's Department for Digital, Culture, Media and Sport, 2018, 4,5).

ومن خلال تتبع الأنظمة والتشريعات واللوائح توصلت الدراسة إلى أن هناك جهودًا كبيرة لتنظيم إنترنت الأشياء على مستوى العالم، إلا أنه لايزال محدودًا ببعض الدول التي يواجه المشرّعون فيها بعض التحديات؛ نظرًا للتطور السريع في تقنيات إنترنت الأشياء. فقد وضعت بعض الدول خططًا وطنية لتنظيم إنترنت الأشياء كدول أمريكا اللاتينية، إلا أنه على النقيض، فإن هناك حكومات أقرت قوانين لمراقبة وجمع بيانات مواطنيهان كهولندا، واليابان (Pedro, 2019).

نتائج الدراسة التحليلية

تضمن هذا الجزء عرضًا إحصائيًا لنتائج الدراسة، اعتمادًا على استجابات الخبراء لكل عبارة من عبارات الاستبانة، مع تفسير هذه النتائج وتحليلها ، وذلك على النحو الآتي:

التساؤل الأول: ما الأنظمة المعمول بها في إنترنت الأشياء على مستوى دول العالم؟

أُستخدم المنهج الوصفي التحليلي لتتبع المواد والقوانين والسياسات والضوابط التي تختص بإنترنت الأشياء التي أقرتها بعض الدول؛ وذلك للإجابة عن هذا التساؤل. وقد وجدت الباحثة عددًا من الأنظمة والتشريعات والسياسات والضوابط التي تم إقرارها في بعض الجوانب؛ حيث إن بعض الدول أقرت بعض القوانين التي تغطي بعض الجوانب، في حين أن دولاً أخرى أصدرت تشريعات وأنظمة ولوائح غطت جوانب أخرى. وقد وجدت الباحثة أن معظم القوانين التي جرى سنَّها في هذا المجال تندرج تحت خمسة جوانب أساسية، وهي:

- الخصوصية.

- الشفافية.
- الأمان.
- جودة البيانات.
- البنية التحتية.

وقد قامت الباحثة بالاعتماد على ما توصلت إليه وعمل قائمة لهذه الجوانب الرئيسة التي جرى ذكرها في الإطار النظري للدراسة، وتتلخص في الجدول رقم (1).

جدول رقم (1): الجوانب الرئيسة لمقترح النظام التشريعي لإنترنت الأشياء بالمملكة العربية السعودية

الجانب	"California's new law SB 327،"	ARTICLE 29 DATA PROTECTION WORKING PARTY in EU	أمان إنترنت الأشياء للمستهلكين في المملكة المتحدة	New Yuruk guidelines	قانون البيانات المفتوحة في مدينة نيويورك	سياسة تصنيف البيانات في مدينة نيويورك	سياسة تشفير البيانات في مدينة نيويورك	قانون حماية الخصوصية الإلكترونية في الاتحاد الأوربي
الخصوصية		✓	✓			✓	✓	✓
الشفافية		✓		✓	✓			
الأمان	✓		✓		✓			
جودة البيانات			✓		✓			
البنية التحتية				✓				

يوضح الجدول رقم (1) القائمة التي تُعدُّ أساسًا لجولات دلفاي التي استخدمتها الباحثة للوصول إلى إجابات السؤال الثاني من أسئلة الدراسة.

التساؤل الثاني: ما مواد القوانين التي ستستخدم في إعداد وبناء النظام التشريعي المقترح لأنظمة إنترنت الأشياء في المملكة العربية السعودية؟

استخدمت الباحثة أسلوب دلفاي للإجابة عن هذا السؤال والأسئلة الفرعية المدرجة، حيث أنه وباستخدام القائمة التي تم إعدادها بالاعتماد على المنهج الوصفي التحليلي، اعتمدت الباحثة على هذه القائمة في الجولة الأولى. ويظهر الجدول رقم (2) نتائج تحليل إجابات الخبراء عن مدى مناسبة كل جانب من الجوانب الرئيسة لمقترح نظام تشريعي لإنترنت الأشياء في المملكة العربية السعودية (الجولة الأولى).

جدول رقم (2): نتائج الجولة الأولى لتقييم الجوانب الرئيسة لمقترح النظام التشريعي لإنترنت الأشياء في المملكة العربية السعودية

الجانب الأول: متطلبات قضايا الخصوصية المحتملة الناشئة من إنترنت الأشياء في المملكة		
المادة	مناسبة العدد	النسبة
1. تصنيف البيانات والمعلومات الشخصية التي يتم جمعها عن طريق إنترنت الأشياء على أنها معلومات خاصة وسرّية.	21	%81
2. إخفاء المعلومات الشخصية بشكل تلقائي من أجهزة إنترنت الأشياء قبل مشاركتها بأي طريقة يمكن أن تجعلها قابلة للبحث أو الاستكشاف.	21	%81
3. الحصول على "موافقة المستخدم" بشكل صحيح وقانوني قبل الشروع في معالجة بياناته الشخصية مع إتاحة الفرصة له بحذفها في أي وقت.	23	%88
4. تهيئة الأجهزة والخدمات؛ بحيث يمكن للمستخدم بسهولة إزالة البيانات الشخصية منها عندما يتم نقل ملكيتها أو عندما يرغب المستخدم في حذفها أو التخلص من الجهاز.	21	%81
5. عدم جمع البيانات إلا لأغراض محددة وصريحة وشرعية، وعدم إعادة معالجتها مرة أخرى بطريقة لا تتوافق مع تلك الأغراض.	20	%77
6. إلغاء تنشيط أو حذف المستخدم عندما يتوقف عن استخدام خدمة ما من خدمات إنترنت الأشياء.	13	%50
7. حفظ البيانات التي يتم جمعها من مستخدمي إنترنت الأشياء داخل حدود المملكة بواسطة مزوّدي خدمات إنترنت الأشياء؛ حفاظًا على أمنها وسرّيتها.	21	%81
8. الحفاظ على سرّية المعلومات التي يتم تبادلها بين الأطراف؛ بحيث لا يتم الكشف عنها لأي شخص آخر غير الأطراف المعنية.	22	%85
9. التأكد من تطبيق الأطراف الأخرى معايير الخصوصية نفسها التي يلتزم بها مزوّد الخدمة نفسه، وذلك عندما يتم مشاركة البيانات أو الاستعانة بمصادر خارجية.	20	%77
10. الجمع والاستخدام والاحتفاظ بالحد الأدنى من البيانات الشخصية الذي يلزم فقط	22	%85

لتقديم الخدمة التي يتوقعها المستخدم.		
الجانب الثاني: متطلبات الشفافية		
العبارة	**مناسبة العدد**	**النسبة**
1. يحق للمستخدم مطالبة الشركة التي تجمع البيانات الشخصية بالإفصاح عن كيفية استخدامها.	19	%73
2. يحق للمستخدم التحكم في ما يخصه من البيانات الشخصية التي تجمعها الشركات.	19	%73
3. يتم دائمًا إشعار المستخدم قبل اتخاذ الخطوات المتعلقة ببياناته الشخصية.	21	%81
4. تلتزم أجهزة إنترنت الأشياء وتطبيقاتها وأنظمتها بالانفتاح والشفافية حول (من وماذا وأين ومتى ولماذا وكيف) تم جمع البيانات ونقلها ومعالجتها واستخدامها.	19	%73
5. تقوم الشركات المصنّعة، ومقدّمو خدمات إنترنت الأشياء، بتزويد المستخدمين بمعلومات واضحة حول أسباب وكيفية استخدام البيانات الخاصة بهم، وذلك لكل خدمة.	20	%77
6. تكون المعلومات المقدّمة للمستخدم موجزة وشفافة ومفهومة، ويمكن الوصول إليها بسهولة.	21	%81
7. تكون سياسة مزوّد خدمة إنترنت الأشياء صريحة وواضحة، ويسهل فهمها من قِبل فرد ذي تعليم متوسط.	19	%73
8. إتاحة البيانات الشخصية التي يتم الحصول عليها بشكل غير مباشر.	16	%62
9. تعريف مستخدمي أجهزة وخدمات إنترنت الأشياء بالمخاطر والقواعد والضمانات والحقوق المتعلقة بمعالجة بياناتهم الشخصية وكيفية ممارسة حقوقهم فيما يتعلق بمثل هذه المعالجة.	24	%92
الجانب الثالث: متطلبات أمان إنترنت الأشياء		
العبارة	**مناسبة العدد**	**النسبة**
1. وضع آلية للمصادقة على الأجهزة المتصلة بإنترنت الأشياء بواسطة مزوّدي خدمات إنترنت الأشياء ومصنّعي أجهزتها.	24	%92
2. وضع كلمة مرور فريدة لكل جهاز يتم تصنيعه.	21	%81
3. وضع نظام لتأمين إنترنت الأشياء وحمايتها من مخاطر: القرصنة- أخطاء النظام - العبث - والمخاطر البيئية.	24	%92
4. وضع آلية لتحديد هويات المستخدمين الذين لديهم إمكانية الوصول إلى أنظمة إنترنت الأشياء ومصادقتها.	24	%92
5. جميع كلمات مرور أجهزة إنترنت الأشياء تكون فريدة، وليست معروفة مثل admin.	23	%88
6. وجود نقطة اتصال عامة بأجهزة إنترنت الأشياء تستخدم بواسطة مصنّعيها في الكشف عن الثغرات الأمنية في أي وقت.	22	%85
7. وجود آلية لمراقبة وتحديد نقاط الضعف الأمنية وتصحيحها -داخل أجهزة إنترنت الأشياء- بواسطة مصنّعي هذه الأجهزة.	25	%96
8. مكونات البرامج في الأجهزة المتصلة بإنترنت الأشياء تكون قابلة للتحديث.	24	%92

9. شروط وفترة استبدال المنتج تكون واضحة للمستخدم، وذلك بالنسبة للأجهزة التي لا يمكن تجديدها.	23	%88
10. ضمان عدم تعديل البيانات من قبل جهة خارجية (بطريق الخطأ أو عن قصد)؛ حفاظًا على أمان بيانات المستخدمين.	24	%92
11. يسمح لمقدّمي شبكات وخدمات إنترنت الأشياء بمعالجة البيانات التي تم جمعها فقط إذا كان ذلك بغرض الحفاظ على أمن شبكات وخدمات إنترنت الأشياء، أو اكتشاف الأخطاء الفنية أو المخاطر الأمنية أو الهجمات.	23	%88
12. يسمح لمقدّمي شبكات وخدمات إنترنت الأشياء بمعالجة البيانات التي تم جمعها إذا كان ذلك بغرض اكتشاف أو منع المخاطر الأمنية أو الهجمات على الأجهزة الطرفية للمستخدمين النهائيين.	25	%96
13. يسمح لمقدّمي شبكات وخدمات إنترنت الأشياء بمعالجة البيانات التي تم جمعها إذا كان ذلك بغرض الامتثال لالتزام قانوني يخضع له المزوّد في المملكة.	23	%88
الجانب الرابع: متطلبات جودة البيانات		
العبارة	**مناسبة العدد**	**النسبة**
1. وجود آلية لمراجعة بيانات إنترنت الأشياء ومراقبتها باستمرار والتأكد من دقتها وصحتها.	23	%88
2. يجب جمع البيانات ذات الصلة بالخدمة المقدّمة من قبل أجهزة إنترنت الأشياء التي تتعلق بالأغراض التي يتم جمعها من أجلها ومعالجتها.	20	%77
3. تحديث البيانات التي يتم جمعها عن طريق أجهزة إنترنت الأشياء؛ لتجنب الأخطاء التي قد تسببها معالجة بيانات قديمة.	24	%92
4. وجود آلية للتأكد من جودة عمل المستشعرات والأجهزة المرتبطة بأجهزة إنترنت الأشياء؛ حتى لا يتم فقد البيانات أو التقليل من كفاءة الأجهزة	24	%92
5. التثبت من مصداقية وموثوقية البيانات التي يتم جمعها من خلال أجهزة إنترنت الأشياء.	21	%81
6. وجود آليات تحقّق تكامل البيانات التي يتم جمعها عن طريق الأجهزة المرتبطة بأنظمة إنترنت الأشياء.	22	%85
7. أرشفة بيانات إنترنت الأشياء بطريقة نظامية لجميع المستخدمين.	20	%77
8. قيام مقدّمي خدمات إنترنت الأشياء بالتحليل الفوري للبيانات التي تم جمعها وتكاملها.	19	%73
الجانب الخامس: متطلبات البنية التحتية		
العبارة	**مناسبة العدد**	**النسبة**
1. الاستفادة من الشبكات اللاسلكية الثابتة الموجودة حاليًا كلما كان ذلك ممكنًا و مناسبًا.	25	%96
2. الاستفادة من العقود أو الاتفاقات التي وقّعتها الدولة كلما كان ذلك ملائمًا.	24	%92
3. تطوير الحلول بشكل تعاوني بين المؤسسات والهيئات والوزارات؛ لتجنب	24	%92

التكرار وتقليل التكلفة.		
4. تحتفظ الهيئة الحكومية المسؤولة بقائمة جرد بأجهزة إنترنت الأشياء المنتشرة في أنحاء الدولة.	21	%81
5. تحتفظ الهيئة الحكومية المسؤولة بقائمة بالأصول العامة أو الخاصة التي يتم تثبيت الأجهزة عليها.	23	%88
6. تحتفظ الهيئة الحكومية المسؤولة بالتفاصيل والمعلومات الخاصة بالشبكات التي تستخدمها أجهزة إنترنت الأشياء.	24	%92
7. تقوم الهيئة الحكومية المسؤولة بنشر معلومات عامة عن أنظمة إنترنت الأشياء (مثل أجهزة استشعار نوعية الهواء).	24	%92
8. وجود اتفاقيات واضحة لترخيص الموقع وشروط الخدمة المقررة لكل أجهزة إنترنت الأشياء ومعدات الشبكات المثبتة من قبل الدولة.	24	%92
9. وسم أجهزة إنترنت الأشياء ومعدات الشبكة بالاسم ومعلومات الاتصال الخاصة بالطرف المسؤول.	25	%96
10. وجود خطط مرنة لأنظمة إنترنت الأشياء تضمن استمرارية الخدمة في حال وقوع الكوارث الطبيعية (مثل الفيضانات الشديدة) أو حالات الطوارئ الأخرى (مثل انقطاع التيار الكهربي).	25	%96
11. وجود القواعد والتنظيمات التي تحكم عمليات صيانة الأصول العامة بما ييسر عمليات الصيانة والإصلاح والاستبدال.	25	%96

يتضح من الجدول رقم (2) نتائج الجولة الأولى على قائمة الجوانب الرئيسة لبناء المقترح ورأي المشاركين، وعددهم (26) خبيرًا، في أسلوب دلفاي على هذه الجوانب. ومن خلال قراءة الجدول، يتضح أن هناك تباينًا واضحًا في موافقة الخبراء على مناسبة العبارات من عدمها. وعليه، فقد قامت الباحثة بالإبقاء على العبارات التي حصلت على نسبة 80% فما فوق، وإعادة صياغة العبارات التي حصلت على نسبة أقل من 80%، وإعادة القائمة للخبراء كجولة ثانية؛ من أجل مراجعة مدى مناسبة العبارات (المواد) في ضوء رأي الخبراء الآخرين. ويظهر الجدول رقم (3) القائمة بعد الأخذ بمقترحات الخبراء وإعادة صياغة بعض العبارات.

جدول رقم (3): قائمة الجوانب الرئيسة لبناء نظام تشريعي لأنظمة إنترنت الأشياء في المملكة العربية السعودية بعد التعديل

الجانب الأول: متطلبات قضايا الخصوصية المحتملة الناشئة من إنترنت الأشياء في المملكة	
المادة	**ملاحظات**
1. تصنيف البيانات والمعلومات الشخصية التي يتم جمعها عن طريق إنترنت الأشياء على أنها معلومات خاصة وسرية.	
2. إخفاء المعلومات الشخصية بشكل تلقائي من أجهزة إنترنت الأشياء قبل مشاركتها بأي طريقة يمكن أن تجعلها قابلة للبحث أو الاستكشاف.	
3. الحصول على "موافقة المستخدم" بشكل صحيح وقانوني قبل الشروع في معالجة بياناته الشخصية مع إتاحة الفرصة له بحذفها في أي وقت.	
4. تهيئة الأجهزة والخدمات؛ بحيث يمكن للمستخدم بسهولة إزالة البيانات الشخصية منها عندما يتم نقل ملكيتها أو عندما يرغب المستخدم في حذفها أو التخلص من الجهاز.	
5. جمع البيانات لأغراض محددة وصريحة، ولا تُعاد معالجتها مرّةً أخرى بطريقة لا تتوافق مع تلك الأغراض.	تم تعديل صياغة العبارة
6. حذف المستخدم عندما يتوقف عن استخدام خدمة ما من خدمات إنترنت الأشياء.	تم تعديل صياغة العبارة
7. حفظ البيانات التي يتم جمعها من مستخدمي إنترنت الأشياء داخل حدود المملكة بواسطة مزوّدي خدمات إنترنت الأشياء؛ حفاظًا على أمنها وسريتها.	
8. الحفاظ على سرية المعلومات التي يتم تبادلها بين الأطراف؛ بحيث لا يتم الكشف عنها لأي شخص آخر غير الأطراف المعنية.	
9. وجود هيئة تراقب تطبيق الأطراف الأخرى لمعايير الخصوصية نفسها التي يلتزم بها مزوّد الخدمة نفسه، وذلك عندما يتم مشاركة البيانات أو الاستعانة بمصادر خارجية.	تم تعديل صياغة العبارة
10. الجمع والاستخدام والاحتفاظ بالحد الأدنى من البيانات الشخصية، الذي يلزم فقط لتقديم الخدمة التي يتوقعها المستخدم.	
الجانب الثاني: متطلبات الشفافية	
العبارة	**ملاحظات**
1. يحق للمستخدم مطالبة الشركات المصنّعة ومقدّمي خدمات إنترنت الأشياء بالإفصاح عن كيفية استخدام البيانات الشخصية التي تم جمعها.	تم تعديل صياغة العبارة
2. يحق للمستخدم دائمًا التحكم في ما يخصه من البيانات الشخصية التي تجمعها الشركات.	تم تعديل صياغة العبارة
3. يتم دائمًا إشعار المستخدم قبل اتخاذ الخطوات المتعلقة ببياناته الشخصية.	
4. تلتزم أجهزة إنترنت الأشياء و تطبيقاتها وأنظمتها بالشفافية الكاملة حول عمليات جمع البيانات ونقلها ومعالجتها واستخدامها.	تم تعديل صياغة العبارة
5. تقوم الشركات المصنّعة، ومقدّمو خدمات إنترنت الأشياء، بتزويد المستخدمين بمعلومات واضحة حول أسباب وكيفية استخدام البيانات التي تم جمعها.	تم تعديل صياغة العبارة

6. تكون المعلومات المقدّمة للمستخدم موجزة وشفافة ومفهومة، ويمكن الوصول إليها بسهولة.	
7. تكون سياسة مزوّد خدمة إنترنت الأشياء صريحة وواضحة، ويسهل فهمها من قِبل جميع أفراد المجتمع.	تم تعديل صياغة العبارة
8. إعلام المستخدم بالبيانات الشخصية التي يتم الحصول عليها بشكل غير مباشر.	تم تعديل صياغة العبارة
9. تعريف مستخدمي أجهزة وخدمات إنترنت الأشياء بالمخاطر والقواعد والضمانات والحقوق المتعلقة بمعالجة بياناتهم الشخصية وكيفية ممارسة حقوقهم فيما يتعلق بمثل هذه المعالجة.	
الجانب الثالث: متطلبات أمان إنترنت الأشياء	
العبارة	**ملاحظات**
1. وضع آلية للمصادقة على الأجهزة المتصلة بإنترنت الأشياء بواسطة مزوّدي خدمات إنترنت الأشياء ومصنّعي أجهزتها.	
2. وضع كلمة مرور فريدة لكل جهاز يتم تصنيعه.	
3. وضع نظام لتأمين إنترنت الأشياء وحمايتها من مخاطر: القرصنة- أخطاء النظام - العبث - والمخاطر البيئية.	
4. وضع آلية لتحديد هويات المستخدمين الذين لديهم إمكانية الوصول إلى أنظمة إنترنت الأشياء ومصادقتها.	
5. جميع كلمات مرور أجهزة إنترنت الأشياء تكون فريدة، وليست معروفة مثل admin.	
6. وجود نقطة اتصال عامة بأجهزة إنترنت الأشياء تستخدم بواسطة مصنّعيها في الكشف عن الثغرات الأمنية في أي وقت.	
7. وجود آلية لمراقبة وتحديد نقاط الضعف الأمنية وتصحيحها - داخل أجهزة إنترنت الأشياء- بواسطة مصنّعي هذه الأجهزة.	
8. مكونات البرامج في الأجهزة المتصلة بإنترنت الأشياء تكون قابلة للتحديث.	
9. شروط وفترة استبدال المنتج تكون واضحة للمستخدم، وذلك بالنسبة للأجهزة التي لا يمكن تجديدها.	
10. ضمان عدم تعديل البيانات من قبل جهة خارجية (بطريق الخطأ أو عن قصد)؛ حفاظًا على أمان بيانات المستخدمين.	
11. يسمح لمقدّمي شبكات وخدمات إنترنت الأشياء بمعالجة البيانات التي تم جمعها فقط إذا كان ذلك بغرض الحفاظ على أمن شبكات وخدمات إنترنت الأشياء، أو اكتشاف الأخطاء الفنية أو المخاطر الأمنية أو الهجمات.	
12. يسمح لمقدّمي شبكات وخدمات إنترنت الأشياء بمعالجة البيانات التي تم جمعها إذا كان ذلك بغرض اكتشاف أو منع المخاطر الأمنية أو الهجمات على الأجهزة الطرفية للمستخدمين النهائيين.	
13. يسمح لمقدّمي شبكات وخدمات إنترنت الأشياء بمعالجة البيانات التي تم جمعها إذا كان ذلك بغرض الامتثال لالتزام قانوني يخضع له المزوّد في المملكة.	

الجانب الرابع: متطلبات جودة البيانات	
العبارة	**ملاحظات**
1. وجود آلية لمراجعة بيانات إنترنت الأشياء ومراقبتها باستمرار والتأكد من دقتها وصحتها.	
2. يجب أن يتم جمع البيانات ذات الصلة بالخدمة المقدّمة من قبل أجهزة إنترنت الأشياء.	تم تعديل صياغة العبارة
3. تحديث البيانات التي يتم جمعها عن طريق أجهزة إنترنت الأشياء؛ لتجنب الأخطاء التي قد تسببها معالجة بيانات قديمة.	
4. وجود آلية للتأكد من جودة عمل المستشعرات والأجهزة المرتبطة بأجهزة إنترنت الأشياء؛ حتى لا يتم فقد البيانات أو التقليل من كفاءة الأجهزة.	
5. التثبت من مصداقية وموثوقية البيانات التي يتم جمعها من خلال أجهزة إنترنت الأشياء.	
6. وجود آليات تحقّق تكامل البيانات التي يتم جمعها عن طريق الأجهزة المرتبطة بأنظمة إنترنت الأشياء.	
7. قيام مزوّدي خدمة إنترنت الأشياء بأرشفة بيانات إنترنت الأشياء التي يتم جمعها بطريقة نظامية لجميع المستخدمين.	تم تعديل صياغة العبارة
8. قيام مقدّمي خدمات إنترنت الأشياء بالتحليل الفوري للبيانات التي تم جمعها لمنع تراكمها.	تم تعديل صياغة العبارة
9. وجود تأمين إجباري على الشركات ومقدّمي الخدمات ضدّ هذه الأخطاء الفنية أو المخاطر أو الهجمات	عبارة جديدة
الجانب الخامس: متطلبات البنية التحتية	
العبارة	**ملاحظات**
1. الاستفادة من الشبكات اللاسلكية والثابتة الموجودة حاليًا كلما كان ذلك ممكنًا و مناسبًا.	
2. الاستفادة من العقود أو الاتفاقات التي وقعتها الدولة كلما كان ذلك ملائمًا.	
3. تطوير الحلول بشكل تعاوني بين المؤسسات والهيئات والوزارات؛ لتجنب التكرار وتقليل التكلفة.	
4. تحتفظ الهيئة الحكومية المسؤولة بقائمة جرد بأجهزة إنترنت الأشياء المنتشرة في أنحاء الدولة.	
5. تحتفظ الهيئة الحكومية المسؤولة بقائمة بالأصول العامة أو الخاصة التي يتم تثبيت الأجهزة عليها.	
6. تحتفظ الهيئة الحكومية المسؤولة بالتفاصيل والمعلومات الخاصة بالشبكات التي تستخدمها أجهزة إنترنت الأشياء.	
7. تقوم الهيئة الحكومية المسؤولة بنشر معلومات عامة عن أنظمة إنترنت الأشياء (مثل أجهزة استشعار نوعية الهواء).	
8. وجود اتفاقيات واضحة لترخيص الموقع وشروط الخدمة المقررة لكل أجهزة إنترنت	

الأشياء ومعدّات الشبكات المثبتة من قبل الدولة.	
9. وسم أجهزة إنترنت الأشياء ومعدّات الشبكة بالاسم ومعلومات الاتصال الخاصة بالطرف المسؤول.	
10. وجود خطط مرنة لأنظمة إنترنت الأشياء تضمن استمرارية الخدمة في حال وقوع الكوارث الطبيعية (مثل الفيضانات الشديدة) أو حالات الطوارئ الأخرى (مثل انقطاع التيار الكهربي).	
11. وجود القواعد والتنظيمات التي تحكم عمليات صيانة الأصول العامة بما ييسر عمليات الصيانة والإصلاح والاستبدال.	

بناءً على التعديل الذي تم على قائمة الجولة الأولى للجوانب الأساسية لبناء نظام تشريعي لأنظمة إنترنت الأشياء في المملكة العربية السعودية، قامت الباحثة بإعداد قائمة لعبارات (مواد) الجوانب الرئيسة للنظام، والتي حصلت على نسبة تكرار 50% و أقل من 80%، بناءً على مقترحات الخبراء واستعدادًا للجولة الثانية، ومن ثمَّ أخذ رأي الخبراء مرّة أخرى؛ للوصول إلى اتفاق جماعي أو نسبة تكرار تساوي أو تزيد عن 80% على العبارات التي لم يتفق عليها بشكل كامل كما هو موضح في الجدول رقم (4).

جدول رقم (4): القائمة الرئيسة لجوانب النظام التشريعي المقترح للجولة الثانية

الجانب الأول: متطلبات قضايا الخصوصية المحتملة الناشئة من إنترنت الأشياء في المملكة			
المادة	**مناسبة**	**غير مناسبة**	**ملاحظات**
1.جمع البيانات لأغراض محددة وصريحة، وألا تُعاد معالجتها مرّة أخرى بطريقة لا تتوافق مع تلك الأغراض.			
2.حذف المستخدم عندما يتوقف عن استخدام خدمة ما من خدمات إنترنت الأشياء.			
3.وجود هيئة تراقب تطبيق الأطراف الأخرى لمعايير الخصوصية نفسها التي يلتزم بها مزوّد خدمة إنترنت الأشياء نفسه، وذلك عندما يتم مشاركة البيانات أو عندما يُستعان بمصادر خارجية.			
الجانب الثاني: متطلبات الشفافية			
العبارة	**مناسبة**	**غير مناسبة**	**ملاحظات**
1.يحق للمستخدم مطالبة الشركات المصنّعة ومقدّمي خدمات إنترنت الأشياء بالإفصاح عن كيفية استخدام البيانات الشخصية التي تم جمعها.			
2.يحق للمستخدم دائمًا التحكم في ما يخصّه من البيانات الشخصية التي			

تجمعها الشركات.			
3.تلتزم أجهزة إنترنت الأشياء و تطبيقاتها وأنظمتها بالشفافية الكاملة حول عمليات جمع البيانات ونقلها ومعالجتها واستخدامها.			
4.تقوم الشركات المصنّعة، ومقدّمو خدمات إنترنت الأشياء، بتزويد المستخدمين بمعلومات واضحة حول أسباب وكيفية استخدام البيانات التي تم جمعها.			
5. تكون سياسة مزوّد خدمة إنترنت الأشياء صريحة وواضحة، ويسهل فهمها من قِبل جميع أفراد المجتمع.			
6.إعلام المستخدم بالبيانات الشخصية التي يتم الحصول عليها بشكل غير مباشر.			
7.تظل الخدمات المقدَّمة من قبل مزوّدي خدمات إنترنت الأشياء متاحة للاستخدام لمن له الحق في ذلك إذا اختار المستهلك مشاركة أو جمع البيانات.			
الجانب الثالث: متطلبات أمان إنترنت الأشياء			
الجانب الرابع: متطلبات جودة البيانات			
العبارة	**مناسبة**	**غير مناسبة**	**ملاحظات**
1.يجب أن يتم فقط جمع البيانات ذات الصلة بالخدمة المقدّمة من قبل أجهزة إنترنت الأشياء.			
2.قيام مزوّدي خدمة إنترنت الأشياء بأرشفة بيانات إنترنت الأشياء التي يتم جمعها بطريقة نظامية لجميع المستخدمين.			
3.قيام مقدّمي خدمات إنترنت الأشياء بالتحليل الفوري للبيانات التي تم جمعها؛ لمنع تراكمها.			
4.وجود تأمين إجباري على شركات ومقدّمي خدمات إنترنت الأشياء ضدّ الأخطاء الفنية أو المخاطر أو الهجمات.			
الجانب الخامس: متطلبات البنية التحتية			

يظهر الجدول رقم (5) نتائج تحليل إجابات الخبراء على القائمة المعدله للنظام التشريعي المقترح لأنظمة إنترنت الأشياء في المملكة العربية السعودية (الجولة الثانية)، البالغ عددهم (24) خبيراً

جدول رقم (5): نتائج الجولة الثانية لتقييم الجوانب الرئيسة لمقترح النظام التشريعي لإنترنت الأشياء في المملكة العربية السعودية

الجانب الأول: متطلبات قضايا الخصوصية المحتملة الناشئة من إنترنت الأشياء في المملكة		
المادة	**مناسبة العدد**	**النسبة**
1. جمع البيانات لأغراض محددة وصريحة، وألا تُعاد معالجتها مرة أخرى بطريقة لا تتوافق مع تلك الأغراض.	22	%92
2. حذف المستخدم عندما يتوقف عن استخدام خدمة ما من خدمات إنترنت الأشياء.	16	%67
3. وجود هيئة تراقب تطبيق الأطراف الأخرى لمعايير الخصوصية نفسها التي يلتزم بها مزوّد خدمة إنترنت الأشياء نفسه، وذلك عندما يتم مشاركة البيانات أو عندما يُستعان بمصادر خارجية.	23	%96
الجانب الثاني: متطلبات الشفافية		
العبارة	**مناسبة العدد**	**النسبة**
1. يحق للمستخدم مطالبة الشركات المصنّعة ومقدّمي خدمات إنترنت الأشياء بالإفصاح عن كيفية استخدام البيانات الشخصية التي تم جمعها.	22	%92
2. يحق للمستخدم دائمًا التحكم في ما يخصه من البيانات الشخصية التي تجمعها الشركات.	23	%96
3. تلتزم أجهزة إنترنت الأشياء وتطبيقاتها وأنظمتها بالشفافية الكاملة حول عمليات جمع البيانات ونقلها ومعالجتها واستخدامها.	23	%96
4. تقوم الشركات المصنّعة، ومقدّو خدمات إنترنت الأشياء، بتزويد المستخدمين بمعلومات واضحة حول أسباب وكيفية استخدام البيانات التي تم جمعها.	20	%83
5. تكون سياسة مزوّد خدمة إنترنت الأشياء صريحة وواضحة، ويسهل فهمها من قِبل جميع أفراد المجتمع.	23	%96

6. إعلام المستخدم بالبيانات الشخصية التي يتم الحصول عليها بشكل غير مباشر.	20	%83
الجانب الثالث: متطلبات أمان إنترنت الأشياء		
الجانب الرابع: متطلبات جودة البيانات		
العبارة	**مناسبة العدد**	**النسبة**
1. يجب أن يتم فقط جمع البيانات ذات الصلة بالخدمة المقدّمة من قبل أجهزة إنترنت الأشياء.	22	%92
2. قيام مزوّدي خدمة إنترنت الأشياء بأرشفة بيانات إنترنت الأشياء التي يتم جمعها بطريقة نظامية لجميع المستخدمين.	20	%83
3. قيام مقدّمي خدمات إنترنت الأشياء بالتحليل الفوري للبيانات التي تم جمعها؛ لمنع تراكمها.	21	%88
4. وجود تأمين إجباري على شركات ومقدّمي خدمات إنترنت الأشياء ضدّ الأخطاء الفنية أو المخاطر أو الهجمات.	23	%96
الجانب الخامس: متطلبات البنية التحتية		

يتضح من الجدول رقم (5) أن هناك إجماعًا من قبل الخبراء المشاركين على معظم العبارات (المواد) التي شملتها الجولة الثانية بنسبة 83% فأكثر، عدا العبارة الثانية من متطلب قضايا الخصوصية المحتملة الناشئة من إنترنت الأشياء في المملكة العربية السعودية التي تنص على (حذف المستخدم عندما يتوقف عن استخدام خدمة ما من خدمات إنترنت الأشياء)؛ فقد حصلت العبارة على موافقة بنسبة 50% في الجولة الأولى، ونسبة موافقة 67% في الجولة الثانية – سيتم تفسيرها لاحقاً في هذا الفصل. وبناءً على ذلك، فقد تم الاكتفاء بهاتين الجولتين من أسلوب دلفاي. وعليه فإن نتائج الإجابة عن السؤال الثاني هي كالآتي:

أ. ما مواد القوانين المتعلقة بجانب الخصوصية؟

تكوّن هذا المتطلب من (10) عبارات –مواد– حيث تم حساب الوزن النسبي والنسبة المئوية وترتيب كل عبارة بناءً على إجابات الخبراء، بالإضافة إلى الدرجة الكلية للجانب، وقد جاءت النتائج مرتبة بحسب أهميتها كما الآتي:

جدول رقم (6): مدى مناسبة مواد القوانين المتعلقة بخصوصية إنترنت الأشياء والنسبة المئوية للعبارات.

الجانب الأول: متطلبات قضايا الخصوصية المحتملة الناشئة من إنترنت الأشياء في المملكة			
المادة	**الوزن النسبي***	**النسبة**	**الترتيب****
1. تصنيف البيانات والمعلومات الشخصية التي يتم جمعها عن طريق إنترنت الأشياء على أنها معلومات خاصة وسرية.	21	%81	5
2. إخفاء المعلومات الشخصية بشكل تلقائي من أجهزة إنترنت الأشياء قبل مشاركتها بأي طريقة يمكن أن تجعلها قابلة للبحث أو الاستكشاف.	21	%81	5
3. الحصول على "موافقة المستخدم" بشكل صحيح وقانوني قبل الشروع في معالجة بياناته الشخصية مع إتاحة الفرصة له بحذفها في أي وقت.	23	%88	3
4. تهيئة الأجهزة والخدمات؛ بحيث يمكن للمستخدم بسهولة إزالة البيانات الشخصية منها عندما يتم نقل ملكيتها أو عندما يرغب المستخدم في حذفها أو التخلص من	21	%81	5

* يُقصد به مجموع عدد الخبراء في كلا الجولتين الذين يرون مناسبة العبارة لتكون جزءً من مواد النظام التشريعي المقترح لأنظمة إنترنت الأشياء في المملكة.

** رتبة كل عبارة بحسب النسبة التي حققتها.

الجهاز.			
5. يتم جمع البيانات لأغراض محددة وصريحة، وألا تُعاد معالجتها مرة أخرى بطريقة لا تتوافق مع تلك الأغراض.	22	%92	2
6. حذف المستخدم عندما يتوقف عن استخدام خدمة ما من خدمات إنترنت الأشياء.	16	%67	6
7. حفظ البيانات التي يتم جمعها من مستخدمي إنترنت الأشياء داخل حدود المملكة بواسطة مزوّدي خدمات إنترنت الأشياء؛ حفاظًا على أمنها وسريتها.	21	%81	5
8. الحفاظ على سرية المعلومات التي يتم تبادلها بين الأطراف؛ بحيث لا يتم الكشف عنها لأي شخص آخر غير الأطراف المعنية.	22	%85	4
9. وجود هيئة تراقب تطبيق الأطراف الأخرى لمعايير الخصوصية نفسها التي يلتزم بها مزوّد خدمة إنترنت الأشياء نفسه، وذلك عندما يتم مشاركة البيانات أو عندما يُستعان بمصادر خارجية.	23	%96	1
10. الجمع والاستخدام والاحتفاظ بالحد الأدنى من البيانات الشخصية، الذي يلزم فقط لتقديم الخدمة التي يتوقعها المستخدم.	22	%85	4
الدرجة الكلية للجانب*	212	%83	

يتضح من الجدول رقم (6) أن الخبراء المشاركين قد اتفقوا بنسبة 81% فأكثر على المواد المتعلقة بخصوصية إنترنت الأشياء المفترض تطبيقها على أنظمة إنترنت الأشياء في المملكة العربية السعودية، عدا المادة التي تنص على أنه (يجب حذف المستخدم عندما

* يُقصد به درجة أهمية الجانب مقارنةً بالجوانب الأخرى المدرجة في الاستبانة.

يتوقف عن استخدام خدمة ما من خدمات إنترنت الأشياء)، والتي حصلت على اتفاق بنسبة 67%، والمستندة للقاعدة رقم (6) من الضوابط التي وضعتها المملكة المتحدة تحت مسمّى (أمان إنترنت الأشياء للمستهلكين) " Consumer Internet of Things (IoT) Security for manufacturers"، الذي ينصُّ على وجوب تقليل منافذ الهجوم في أنظمة إنترنت الأشياء، ومنها حذف المستخدم عندما يتوقف عن استخدام أحد خدمات إنترنت الأشياء، وكذلك المادة رقم (7) من قانون حماية الخصوصية الإلكترونية EU/0003/2017 والتي تنصُّ على أنه يجب إلغاء تنشيط المستخدم كلياً عندما يتوقف عن استخدام أي خدمة من خدمات إنترنت الأشياء. وعليه ترى الباحثة وجوب إضافتها في المقترح.

وبالنسبة لبقية العبارات، فمن الملاحظ أن العبارة رقم (9) حصلت على نسبة اتفاق عالية 96%، واستندت إلى القاعدة رقم (67) في اللائحة التنفيذية التي قدمتها فرقة العمل العاملة بموجب المادة 29 ARTICLE 29 DATA PROTECTION WORKING PARTY التي تقضي بوجوب الالتزام بمعايير الخصوصية من قبل مزوّد خدمة إنترنت الأشياء وكل من له الإذن بمشاركة بيانات المستخدمين. أما العبارة رقم (5) فقد حصلت على نسبة 92%، واستندت إلى سياسة تصنيف البيانات في مدينة نيويورك التي تشدد على وجوب جمع البيانات مقابل خدمة ما، وأن يتم معالجتها من أجل تلك الخدمة فقط. أما العبارة رقم (3) التي حصلت على موافقة بنسبة 88% من مجموعة الخبراء، فقد استندت إلى القاعدة رقم (8) من ضوابط أمان إنترنت الأشياء للمستهلكين التي وضعتها المملكة المتحدة، والتي تؤكد ضرورة الحصول على موافقة المستخدم بطريقة قانونية قبل جمع بياناته ومعالجتها، مع إعطائه الحق بحذفها متى ما أراد.

أما العبارات رقم (8– 10) فقد حصلت على إجماع الخبراء بنسبة 85%، وقد استندت العبارة رقم (8) إلى المادة رقم (5) من قانون حماية الخصوصية الإلكترونية EU/0003/2017 التي تنصُّ على أنه لا يجوز كشف بيانات المستخدمين وتبادلها إلا لمن

له الحق في ذلك، والعبارة رقم (10) استندت إلى القاعدة رقم (8) من ضوابط أمان إنترنت الأشياء للمستهلكين التي وضعتها المملكة المتحدة، والتي أكدت على أن مقدم الخدمة يلزمه الحصول على الحد الأدنى الموجب لتقديم الخدمة للمستخدم.

أما العبارات رقم (1-2-4-7) فقد حصلت على اتفاق بنسبة 81%، واستندت العبارة رقم (1) إلى سياسة تصنيف البيانات في مدينة نيويورك التي صنفت بيانات إنترنت الأشياء بالسرية. أما العبارة رقم (2) فاستندت إلى سياسة تشفير البيانات في مدينة نيويورك التي تنص على أن البيانات الشخصية يجب أن يتم إخفاؤها بشكل تلقائي؛ حتى لا يمكن كشفها من قبل الآخرين، وتصبح بيانات المستخدم عرضة للاستخدام لغير الغرض الذي جمعت لأجله. والعبارة رقم (4) استندت إلى القاعدة رقم (11) من ضوابط أمان إنترنت الأشياء للمستهلكين التي وضعتها المملكة المتحدة التي تعطي الحق للمستخدم بإمكانية حذف بياناته وإزالتها عندما يرغب بالتخلص من الجهاز أو بيعه. وبالنسبة للعبارة رقم (7) فقد استندت إلى المادة رقم (2) من قانون حماية الخصوصية الإلكترونية EU/0003/2017 التي أكّدت على ضرورة حفظ البيانات التي يتم جمعها من المستخدم في قواعد بيانات داخل حدود الدولة التي يسكنها؛ حفاظًا على سرية معلوماته وأمنها.

وبالنظر للدرجة الكلية والوزن النسبي في الجدول رقم (6)، يتضح أن جانب الخصوصية حصل على درجة كلية تساوي 212، ووزن نسبي بمقدار 83%، وعليه، فإن جانب الخصوصية يأتي في المرتبة الرابعة في الأهمية من بين مراتب الجوانب الأساسية لأنظمة إنترنت الأشياء (الخصوصية- الشفافية- الأمان- جودة البيانات- البنية التحتية).

ب. ما مواد القوانين المتعلقة بجانب الشفافية؟

تكوّن هذا السؤال من (9) عبارات –مواد– حيث تم حساب الوزن النسبي والنسبة المئوية وترتيب كل عبارة بناءً على إجابات الخبراء، بالإضافة إلى الدرجة الكلية للجانب، وقد جاءت النتائج مرتبة بحسب أهميتها كما الآتي:

جدول رقم (7): مدى مناسبة مواد القوانين المتعلقة بمتطلبات شفافية أنظمة إنترنت الأشياء والنسبة المئوية للعبارات.

الجانب الثاني: متطلبات الشفافية			
العبارة	**الوزن النسبي***	**النسبة**	**الترتيب****
1. يحق للمستخدم مطالبة الشركات المصنّعة ومقدمي خدمات إنترنت الأشياء بالإفصاح عن كيفية استخدام البيانات الشخصية التي تم جمعها.	22	%92	2
2. يحق للمستخدم دائمًا التحكم في ما يخصه من البيانات الشخصية التي تجمعها الشركات.	23	%96	1
3. يتم دائمًا إشعار المستخدم قبل اتخاذ الخطوات المتعلقة ببياناته الشخصية.	21	%81	4
4. تلتزم أجهزة إنترنت الأشياء وتطبيقاتها وأنظمتها بالشفافية الكاملة حول عمليات جمع البيانات ونقلها ومعالجتها واستخدامها.	23	%96	1
5. تقوم الشركات المصنّعة، ومقدّمو خدمات إنترنت الأشياء، بتزويد المستخدمين بمعلومات واضحة حول أسباب وكيفية استخدام	20	%83	3

* يُقصد به مجموع عدد الخبراء في كلا الجولتين الذين يرون مناسبة العبارة لتكون جزءً من مواد النظام التشريعي المقترح لأنظمة إنترنت الأشياء في المملكة.

** رتبة كل عبارة بحسب النسبة التي حققتها.

البيانات التي تم جمعها.			
6. تكون المعلومات المقدَّمة للمستخدم موجزة وشفافة ومفهومة ويمكن الوصول إليها بسهولة.	21	%81	4
7. تكون سياسة مزوّد خدمة إنترنت الأشياء صريحة وواضحة، ويسهل فهمها من قِبل جميع أفراد المجتمع.	23	%96	1
8. إعلام المستخدم بالبيانات الشخصية التي يتم الحصول عليها بشكل غير مباشر.	20	%83	3
9. تعريف مستخدمي أجهزة وخدمات إنترنت الأشياء بالمخاطر والقواعد والضمانات والحقوق المتعلقة بمعالجة بياناتهم الشخصية وكيفية ممارسة حقوقهم فيما يتعلق بمثل هذه المعالجة.	24	%92	2
الدرجة الكلية للجانب*	189	%89	

يتضح من الجدول رقم (7) أن الخبراء المشاركين قد اتفقوا بنسبة 81% فأكثر على المواد المتعلقة بمتطلب شفافية إنترنت الأشياء؛ فقد جاءت العبارات رقم (2-4-7) بإجماع مجموعة الخبراء بنسبة 96%، وقد استندت العبارة رقم (2) إلى الضوابط المتعلقة بالشفافية بموجب اللائحة 679/2016 رقم (39) الذي يشير إلى وجوب إتاحة وصول المستخدمين إلى بياناتهم الشخصية والتحكم فيها بغض النظر عن كيفية استخدامهم للخدمة. أما العبارة رقم (4) فاستندت إلى الضوابط التي طرحتها مدينة نيويورك، والتي نصت على أنه يجب على مقدمي خدمات إنترنت الأشياء ومصنّعي الأجهزة إيضاح طريقة جمع البيانات وكيفية انتقالها وأسلوب المعالجة الذي سيتم عليها وهدف استخدامها للمستخدم النهائي. وبالنسبة للعبارة رقم (7) فقد استندت إلى الضوابط المتعلقة بالشفافية بموجب اللائحة 679/2016 رقم (9) الذي يؤكد على وجوب توفير معلومات عن الطريقة التي سيتم من خلالها جمع ومعالجة

* يُقصد به درجة أهمية الجانب مقارنةً بالجوانب الأخرى المدرجة في الاستبانة.

واستخدام البيانات التي يتم جمعها من قبل أجهزة الإنترنت للمستخدم بأسلوب صريح مفهوم وغير مبهم ويسهل فهمه من قبل أفراد المجتمع.

تأتي العبارات رقم (1–9) بنسبة إجماع 92%؛ فقد استندت العبارة رقم (1) إلى الضوابط المتعلقة بالشفافية بموجب اللائحة 679/2016 رقم (41) الذي يؤكد على أنه يحق للمستخدم معرفة كيفية استخدام بياناته الشخصية التي يتم جمعها من قبل مزوّدي الخدمات ومصنّعي أجهزة إنترنت الأشياء. أما العبارة رقم (9) فقد استندت إلى الضوابط المتعلقة بالشفافية بموجب اللائحة 679/2016 رقم (10) الذي يفسر المادتين (13 –14) من اللائحة العامة لحماية البيانات التي تنص على أنه يجب على مزوّدي خدمات إنترنت الأشياء الإفصاح عن أهم النتائج المترتبة على معالجة بيانات مستخدمي هذه الخدمات، وذكر نوع التأثير الذي ستحدثه معالجة بياناتهم، كما أنه يجب إيضاح حقوقهم المتعلقة بنتائج هذه المعالجة.

والعبارات رقم (5–8) فقد اتفق الخبراء المشاركون على مدى مناسبتها بنسبة 83%؛ حيث استندت العبارة رقم (5) إلى الضوابط المتعلقة بالشفافية بموجب اللائحة 679/2016 رقم (13) الذي تفسر المادة رقم (12) من اللائحة العامة لحماية البيانات، والتي تنص على ضرورة إفادة المستفيدين بمعلومات واضحة حول أسباب جمع بياناتهم والغرض منها. أما العبارة رقم (8) فقد استندت إلى الضوابط المتعلقة بالشفافية بموجب اللائحة 679/2016 رقم (21) الذي يؤكد على وجوب إطلاع مستخدمي خدمات إنترنت الأشياء على جميع بياناتهم الشخصية التي جُمعت بالطريقة غير المباشرة.

والعبارات رقم (3–6) جاءت بإجماع بنسبة 81%؛ فقد استندت العبارة رقم (3) إلى الضوابط المتعلقة بالشفافية بموجب اللائحة 679/2016 رقم (30) الذي يؤكد على أن للمستخدم الحق في معرفة أي إجراء يتم على بياناته الشخصية التي تم جمعها من قبل أجهزة إنترنت الأشياء قبل معالجتها، ويجب أن يتم إطلاع المستخدم على هذه الإجراءات عند قبول

الخدمة المقدّمة. والعبارة رقم (6) استندت إلى الضوابط المتعلقة بالشفافية بموجب اللائحة 679/2016 رقم (8) الذي يفسر المادة رقم (12.1) من اللائحة العامة لحماية البيانات التي تنص على أن الإجراءات التي ستتم على بيانات مستخدمي إنترنت الأشياء، يجب أن تتم بكفاءة، وتذكر بلغة واضحة ومفهومة، مع إمكانية وصول المستخدم لهذه البيانات بسهولة.

وبالنظر للدرجة الكلية والوزن النسبي في الجدول رقم (7)، يتضح أن جانب الشفافية حصل على درجة كلية تساوي 189، ووزن نسبي بمقدار 89%، وعليه، فإن جانب الشفافية يأتي في المرتبة الثالثة في الأهمية من بين مراتب الجوانب الأساسية لأنظمة إنترنت الأشياء (الخصوصية– الشفافية– الأمان– جودة البيانات– البنية التحتية).

ج. ما مواد القوانين المتعلقة بجانب الأمان؟

تكوّن هذا السؤال من (13) عبارة –مادة– حيث تم حساب الوزن النسبي والنسبة المئوية وترتيب كل عبارة بناءً على إجابات الخبراء، بالإضافة إلى الدرجة الكلية للجانب، وقد جاءت النتائج مرتبة بحسب أهميتها كما الآتي:

جدول رقم (8): مدى مناسبة مواد القوانين المتعلقة بمتطلبات أمان إنترنت الأشياء والنسبة المئوية للعبارات.

الجانب الثالث: متطلبات أمان إنترنت الأشياء			
العبارة	الوزن النسبي*	النسبة	الترتيب**
1. وضع آلية للمصادقة على الأجهزة المتصلة بإنترنت الأشياء بواسطة مزوّدي خدمات إنترنت الأشياء ومصنّعي أجهزتها.	24	%92	2
2. وضع كلمة مرور فريدة لكل جهاز يتم تصنيعه.	21	%81	5
3. وضع نظام لتأمين إنترنت الأشياء وحمايتها من مخاطر: القرصنة– أخطاء النظام –العبث – والمخاطر البيئية.	24	%92	2
4. وضع آلية لتحديد هويات المستخدمين الذين لديهم إمكانية الوصول إلى أنظمة إنترنت الأشياء و مصادقتها.	24	%92	2
5. جميع كلمات مرور أجهزة إنترنت الأشياء تكون فريدة وليست معروفة مثل admin.	23	%88	3
6. وجود نقطة اتصال عامة بأجهزة إنترنت الأشياء تستخدم بواسطة مصنّعيها في الكشف عن الثغرات الأمنية في أي وقت.	22	%85	4
7. وجود آلية لمراقبة وتحديد نقاط الضعف الأمنية وتصحيحها – داخل أجهزة إنترنت الأشياء– بواسطة مصنّعي هذه الأجهزة.	25	%96	1
8. مكونات البرامج في الأجهزة المتصلة بإنترنت الأشياء تكون قابلة للتحديث.	24	%92	2
9. شروط وفترة استبدال المنتج تكون واضحة للمستخدم، وذلك بالنسبة للأجهزة التي لا يمكن تجديدها.	23	%88	3
10. ضمان عدم تعديل البيانات من قبل جهة خارجية (بطريق الخطأ	24	%92	2

* يُقصد به مجموع عدد الخبراء في كلا الجولتين الذين يرون مناسبة العبارة لتكون جزءً من مواد النظام التشريعي المقترح لأنظمة إنترنت الأشياء في المملكة.

** رتبة كل عبارة بحسب النسبة التي حققتها.

أو عن قصد)؛ حفاظًا على أمان بيانات المستخدمين.			
11. يسمح لمقدمي شبكات وخدمات إنترنت الأشياء بمعالجة البيانات التي تم جمعها فقط إذا كان ذلك بغرض الحفاظ على أمن شبكات وخدمات إنترنت الأشياء، أو اكتشاف الأخطاء الفنية أو المخاطر الأمنية أو الهجمات.	23	%88	3
12. يسمح لمقدّمي شبكات وخدمات إنترنت الأشياء بمعالجة البيانات التي تم جمعها إذا كان ذلك بغرض اكتشاف أو منع المخاطر الأمنية أو الهجمات على الأجهزة الطرفية للمستخدمين النهائيين.	25	%96	1
13. يسمح لمقدمي شبكات وخدمات إنترنت الأشياء بمعالجة البيانات التي تم جمعها إذا كان ذلك بغرض الامتثال لالتزام قانوني يخضع له المزوّد في المملكة.	23	%88	3
الدرجة الكلية للجانب*	305	%90	

يتضح من الجدول رقم (8) أن الخبراء قد اتفقوا بنسبة 81% وأكثر على مدى مناسبة مواد هذا الجانب؛ إذ حصلت العبارتان رقم (7–12) على أعلى نسبة؛ حيث اتفق 96% من مجموعة الخبراء المشاركين في الدراسة على مناسبة إدراجهما في المقترح. فقد استندت العبارة رقم (7) إلى قانون كاليفورنيا رقم SB327 الذي ركز على أهمية تحديد وتصحيح نقاط الضعف الأمنية في أجهزة إنترنت الأشياء. أما العبارة رقم (12) فقد استندت إلى القاعدة رقم (2) من ضوابط أمان إنترنت الأشياء للمستهلكين التي وضعتها المملكة المتحدة للحفاظ على أجهزة وبيانات المستخدمين من التهديدات الأمنية واكتشافها قبل وقوعها، التي أكدت على أهمية معالجة البيانات بهدف اكتشاف ومنع أي مشكلة أمنية قد تؤثر على أجهزة المستخدمين.

* يُقصد به درجة أهمية الجانب مقارنةً بالجوانب الأخرى المدرجة في الاستبانة.

بالنسبة للعبارات رقم (1–3–4–8–10) فقد أجمع 92% من الخبراء على أهميتها. واستندت العبارة رقم (1) إلى قانون كاليفورنيا رقم SB327 الذي فرض على مزوّدي خدمات إنترنت الأشياء ومصنّعيها وجوب وضع طريقة معيّنة للمصادقة؛ للحفاظ على أمان أجهزة المستخدمين. أما العبارة رقم (3– 4) فقد استندت إلى اللائحة التنفيذية لقانون البيانات المفتوحة في مدينة نيويورك رقم 2012/011 الذي يدعو لضرورة تأمين أجهزة إنترنت الأشياء من المخاطر والعبث، وقد استندت العبارة رقم (8) إلى القاعدة رقم (3) من ضوابط أمان إنترنت الأشياء للمستهلكين التي وضعتها المملكة المتحدة، والتي نصّت على أنه يجب تحديث مكونات البرامج في الأجهزة المتصلة بالإنترنت بأمان، أن تكون هذه التحديثات في الوقت المناسب وأن لا تؤثر على عمل الجهاز، في حين استندت العبارة رقم (10) إلى قانون كاليفورنيا رقم SB327 الذي وُضع لحماية أمان بيانات المستخدمين وأكد على وجوب حماية بيانات المستخدمين من التعديل.

ومن الملاحظ أن العبارات رقم (5–9–11–13) قد جاءت في الترتيب الثالث في الأهمية في هذا الجانب؛ إذ حصلت على إجماع بنسبة 88%، وقد استمدت العبارة رقم (5) من قانون كاليفورنيا رقم SB327 الذي يؤكد على أنه يجب على المستخدمين اختيار كلمات مرور معقّده نوعًا ما؛ للحفاظ على أجهزتهم من الاختراق. أما العبارة رقم (9) فقد استندت إلى القاعدة رقم (3) من ضوابط أمان إنترنت الأشياء للمستهلكين التي وضعتها المملكة المتحدة، التي شددت بوجوب توضيح إجراءات استبدال أجهزة إنترنت الأشياء التي لا يمكن تحديثها للمستخدم. وأما العبارتان رقم (11–13) فقد استندت إلى القاعدة رقم (2) من ضوابط أمان إنترنت الأشياء للمستهلكين التي وضعتها المملكة المتحدة؛ للحفاظ على أجهزة وبيانات المستخدمين من التهديدات الأمنية واكتشافها قبل وقوعها.

وقد حصلت العبارة رقم (6) على اتفاق بنسبة 85%، واستندت إلى القاعدة رقم (2) من ضوابط أمان إنترنت الأشياء للمستهلكين التي وضعتها المملكة المتحدة، وأكدت على أنه يجب على جميع الشركات التي توفر الأجهزة والخدمات المتصلة بالإنترنت توفير نقطة اتصال عامة كجزء من سياسة الكشف عن الثغرات الأمنية حتى يتمكن الباحثين الأمنيين وغيرهم من الإبلاغ عن المشكلات في الوقت المناسب.

أما العبارة رقم (2) فجاءت في الترتيب الأخير بنسبة اتفاق 81%، واستندت إلى قانون كاليفورنيا رقم SB327 الذي يشدد على مصنّعي أجهزة إنترنت الأشياء بوضع كلمة مرور مختلفة لكل جهاز يتم تصنيعه.

وبالنظر للدرجة الكلية والوزن النسبي في الجدول رقم (8)، يتضح أن جانب الأمان حصل على درجة كلية تساوي 305، ووزن نسبي بمقدار 90%، وعليه، فإن جانب الأمان يأتي في المرتبة الثانية في الأهمية من بين مراتب الجوانب الأساسية لأنظمة إنترنت الأشياء (الخصوصية– الشفافية– الأمان– جودة البيانات– البنية التحتية).

د. ما مواد القوانين المتعلقة بجودة البيانات؟

تكوّن هذا الجانب من (9) عبارات –مواد– حيث تم حساب الوزن النسبي والنسبة المئوية وترتيب كل عبارة بناءً على إجابات الخبراء، بالإضافة إلى الدرجة الكلية للجانب، وقد جاءت النتائج مرتبة بحسب أهميتها كما الآتي:

جدول رقم (9): مدى مناسبة مواد القوانين المتعلقة بمتطلبات جودة بيانات إنترنت الأشياء والنسبة المئوية للعبارات.

الجانب الرابع: متطلبات جودة البيانات			
العبارة	**الوزن النسبي***	**النسبة**	**الترتيب****
1. وجود آلية لمراجعة بيانات إنترنت الأشياء ومراقبتها باستمرار والتأكد من دقتها وصحتها.	23	%88	3
2. يجب أن يتم فقط جمع البيانات ذات الصلة بالخدمة المقدّمة من قبل أجهزة إنترنت الأشياء.	22	%92	2
3. تحديث البيانات التي يتم جمعها عن طريق أجهزة إنترنت الأشياء لتجنب الأخطاء التي قد تسببها معالجة بيانات قديمة.	24	%92	2
4. وجود آلية للتأكد من جودة عمل المستشعرات والأجهزة المرتبطة بأجهزة إنترنت الأشياء؛ حتى لا يتم فقد البيانات أو التقليل من كفاءة الأجهزة.	24	%92	2
5. التثبت من مصداقية وموثوقية البيانات التي يتم جمعها من خلال أجهزة إنترنت الأشياء.	21	%81	6
6. وجود آليات تحقق تكامل البيانات التي يتم جمعها عن طريق الأجهزة المرتبطة بأنظمة إنترنت الأشياء.	22	%85	
7. قيام مزوّدي خدمة إنترنت الأشياء بأرشفة بيانات إنترنت الأشياء التي يتم جمعها بطريقة نظامية لجميع	20	%83	5

* يُقصد به مجموع عدد الخبراء في كلا الجولتين الذين يرون مناسبة العبارة لتكون جزءً من مواد النظام التشريعي المقترح لأنظمة إنترنت الأشياء في المملكة.

** رتبة كل عبارة بحسب النسبة التي حققتها.

المستخدمين.			
8. قيام مقدّمي خدمات إنترنت الأشياء بالتحليل الفوري للبيانات التي تم جمعها؛ لمنع تراكمها.	21	%88	3
9. وجود تأمين إجباري على شركات ومقدّمي خدمات إنترنت الأشياء ضدّ الأخطاء الفنية أو المخاطر أو الهجمات.	23	%96	1
الدرجة الكلية للجانب*	200	%89	

يتضح من الجدول رقم (9) أن الخبراء المشاركين قد اتفقوا بنسبة 81% فأكثر على المواد المتعلقة بجودة بيانات إنترنت الأشياء المفترض تطبيقها على أنظمة إنترنت الأشياء في المملكة العربية السعودية، وقد جاءت العبارة رقم (9) كأعلى العبارات نسبة؛ حيث حصلت على إجماع بنسبة 96%، وهي مقترح اقترحه مجموعة من الخبراء المشاركين؛ حيث أكدوا على ضرورة وجود تأمين يجبر عليه مزوّدي خدمات إنترنت الأشياء ومصنّعي الأجهزة في المملكة العربية السعودية ضدّ الأخطاء المصنعية والهجمات الأمنية والمخاطر البيئية.

أما العبارات رقم (2-3-4) فقد حصلت على اتفاق بنسبة 92%، واُستمدت هذه العبارات الثلاثة من اللائحة التنفيذية لقانون البيانات المفتوحة في مدينة نيويورك رقم 2012/011 التي أوضحت أهمية البيانات وتأثيرها على جودة الخدمة المقدّمة ؛ حيث أكدت اللائحة على أنه يجب جمع البيانات المتعلقة بالخدمة فقط، وتتم معالجتها فورًا؛ منعًا لوقوع الأخطاء التي قد تتسبب فيها بيانات قديمة تم جمعها سابقًا. كما بيّنت أنه يتوجّب وجود آلية واضحة لعمل المستشعرات والأجهزة المتعلقة بجمع بيانات إنترنت الأشياء؛ لرفع كفاءة وجودة البيانات التي يتم جمعها، وبالتالي جودة الخدمة المقدّمة.

* يُقصد به درجة أهمية الجانب مقارنةً بالجوانب الأخرى المدرجة في الاستبانة.

جاءت العبارات رقم (1–8) في الترتيب الثالث في الأهمية، وحصلت على اتفاق بنسبة 88% من مجموعة الخبراء المشاركين، وتطرقت لأهمية وجود طريقة لمراجعة بيانات إنترنت الأشياء قبل معالجتها لاتخاذ القرار المناسب. أما العبارة رقم (6) فقد حصلت على نسبة 85%، في حين حصلت العبارة رقم (7) على نسبة 83%، وقد استندت هذه العبارات (1–6–7–8) إلى اللائحة التنفيذية لقانون البيانات المفتوحة في مدينة نيويورك رقم 2012/011 التي ركّزت على ضرورة التأكّد من صحة البيانات ودقّتها وتكاملها وتحليلها فور جمعها؛ منعًا لتراكمها ومن ثمَّ أرشفتها. أما العبارة رقم (5) فقد حصلت على اتفاق بنسبة 81%، واستندت هذه العبارة إلى القاعدة رقم (10) من ضوابط أمان إنترنت الأشياء للمستهلكين التي وضعتها المملكة المتحدة التي نصّت على وجوب التأكد من صدق البيانات التي يتم جمعها من مستشعرات أجهزة إنترنت الأشياء التي لها تأثير كبير في أسلوب المعالجة المطبّق عليها وجودة المخرجات.

وبالنظر للدرجة الكلية والوزن النسبي في الجدول رقم (9)، يتضح أن جانب جودة البيانات حصل على درجة كلية تساوي 200، ووزن نسبي بمقدار 89%، وعليه، فإن جانب جودة البيانات يأتي في المرتبة الثالثة في الأهمية من بين مراتب الجوانب الأساسية لأنظمة إنترنت الأشياء (الخصوصية– الشفافية– الأمان– جودة البيانات– البنية التحتية)، بالإضافة إلى جانب الشفافية.

هـ. ما مواد القوانين المتعلقة بالبنية التحتية؟

تكوّن هذا الجانب من (11) عبارات –مواد– حيث تم حساب الوزن النسبي والنسبة المئوية وترتيب كل عبارة بناءً على إجابات الخبراء، بالإضافة إلى الدرجة الكلية للجانب، وقد جاءت النتائج مرتبة بحسب أهميتها كما الآتي:

جدول رقم (10): مدى مناسبة مواد القوانين المتعلقة بمتطلبات البنية التحتية لإنترنت الأشياء والنسبة المئوية للعبارات.

الجانب الخامس: متطلبات البنية التحتية			
العبارة	**الوزن النسبي***	**النسبة**	**الترتيب****
1. الاستفادة من الشبكات اللاسلكية والثابتة الموجودة حاليًا كلما كان ذلك ممكنًا و مناسبًا.	25	%96	1
2. الاستفادة من العقود أو الاتفاقات التي وقّعتها الدولة كلما كان ذلك ملائمًا.	24	%92	2
3. تطوير الحلول بشكل تعاوني بين المؤسسات والهيئات والوزارات؛ لتجنب التكرار وتقليل التكلفة.	24	%92	2
4. تحتفظ الهيئة الحكومية المسؤولة بقائمة جرد بأجهزة إنترنت الأشياء المنتشرة في أنحاء الدولة.	21	%81	4
5. تحتفظ الهيئة الحكومية المسؤولة بقائمة الأصول العامة أو الخاصة التي يتم تثبيت الأجهزة عليها.	23	%88	3
6. تحتفظ الهيئة الحكومية المسؤولة بالتفاصيل والمعلومات الخاصة بالشبكات التي تستخدمها أجهزة إنترنت الأشياء.	24	%92	2
7. تقوم الهيئة الحكومية المسؤولة بنشر معلومات عامة عن أنظمة إنترنت الأشياء (مثل أجهزة استشعار نوعية الهواء).	24	%92	2
8. وجود اتفاقيات واضحة لترخيص الموقع وشروط الخدمة المقررة لكل أجهزة إنترنت الأشياء ومعدّات الشبكات المثبتة من قبل الدولة.	24	%92	2
9. وسم أجهزة إنترنت الأشياء ومعدات الشبكة بالاسم	25	%96	1

* يُقصد به مجموع عدد الخبراء في كلا الجولتين الذين يرون مناسبة العبارة لتكون جزءً من مواد النظام التشريعي المقترح لأنظمة إنترنت الأشياء في المملكة.

** رتبة كل عبارة بحسب النسبة التي حققتها.

ومعلومات الاتصال الخاصة بالطرف المسؤول.			
10. وجود خطط مرنة لأنظمة إنترنت الأشياء تضمن استمرارية الخدمة في حال وقوع الكوارث الطبيعية، (مثل الفيضانات الشديدة) أو حالات الطوارئ الأخرى، (مثل انقطاع التيار الكهربي).	25	%96	1
11. وجود القواعد والتنظيمات التي تحكم عمليات صيانة الأصول العامة بما ييسر عمليات الصيانة والإصلاح والاستبدال.	25	%96	1
الدرجة الكلية للجانب*	264	%92	

يتضح من الجدول رقم (10) أن الخبراء المشاركين قد اتفقوا بنسبة 81% فأكثر على المواد المتعلقة بمتطلب البنية التحتية لإنترنت الأشياء؛ فقد جاءت العبارات رقم (1-9-10-11) كأكثر العبارات نسبة في الاتفاق، وقد بلغت نسبة الاتفاق 96% من مجموعة الخبراء المشاركين، وقد استندت هذه العبارات إلى الضوابط التي طرحتها مدينة نيويورك، والتي ركّزت على ضرورة تهيئة البنية التحتية لإنترنت الأشياء والاستفادة من جميع شبكات الإنترنت سواءً الثابتة أو اللاسلكية، كما أكّدت على ضرورة تسجيل معلومات كل جهاز ومقدّم الخدمة التابع له؛ لسهولة تصنيفها، وضرورة وجود قواعد واضحة لتسهيل صيانة هذه الأجهزة وإصلاحها. وأكدت هذه الضوابط وجوب طرح خططٍ تضمن استمرارية خدمات إنترنت الأشياء في حال انقطاع الخدمات لأي ظرفٍ طارئ.

تأتي العبارات رقم (2-3-6-7-8) في المرتبة الثانية في الأهمية؛ حيث حصلت العبارات على اتفاق بنسبة 92%، وقد استندت إلى مجموعة الضوابط التي طرحتها مدينة نيويورك، والتي ركزت على أهمية الاستفادة من العقود التي وقعتها الدولة وتطوير الحلول بين المؤسسات والهيئات والوزارات لتقليل التكلفة؛ من أجل الارتقاء بجودة الخدمات المقدّمة، كما

* يُقصد به درجة أهمية الجانب مقارنةً بالجوانب الأخرى المدرجة في الاستبانة.

أنها أشارت لضرورة احتفاظ الهيئة الحكومية المسؤولة بجميع التفاصيل المتعلقة بشبكات مزوّدي خدمات إنترنت الأشياء، وأن تقوم هذه الهيئة بنشر معلومات عن جميع أنظمة إنترنت الأشياء المستخدمة في المدن كأجهزة الاستشعار الخاصة بدرجة الحرارة وغيرها. فضلاً عن ذلك، أكدت هذه الضوابط على ضرورة وضع شروط وتراخيص لمواقع أجهزة إنترنت الأشياء المثبتة في المدن التابعة للدولة.

أما العبارة رقم (5)، والعبارة رقم (4) فقد حصلتا على إجماع بنسبة 88%، 81% على التوالي، وقد استندتا إلى ضوابط البنية التحتية التي طرحتها مدينة نيويورك، والتي أكدت على وجوب التزام الهيئة المسؤولة بقائمة جميع الأصول سواءً العامة أو الخاصة التي يتم تثبيت أجهزة إنترنت الأشياء عليها، كما يجب أن تحتفظ الهيئة بقائمة جرد لكل أجهزة إنترنت الأشياء الموجودة داخل الدولة.

وبالنظر للدرجة الكلية والوزن النسبي في الجدول رقم (10)، يتضح أن جانب البنية التحتية حصل على درجة كلية تساوي 264، ووزن نسبي بمقدار 92%، وعليه، فإن جانب البنية التحتية يأتي في المرتبة الأولى في الأهمية من بين مراتب الجوانب الأساسية لأنظمة إنترنت الأشياء (الخصوصية– الشفافية– الأمان– جودة البيانات– البنية التحتية).

تلاحظ الباحثة من الجداول رقم (6–7–8–9–10) المذكورة آنفاً، أن جانب البنية التحتية لإنترنت الأشياء جاء كأهم جانب بنسبة 92%، يليه متطلب أمان إنترنت الأشياء بنسبة 90%. أما متطلب شفافية إنترنت الأشياء وجودة بيانات إنترنت الأشياء، فقد جاء في المرتبة الثالثة من الأهمية بنسبة 89%، وجاء متطلب خصوصية إنترنت الأشياء بنسبة 83%. ويتضح أن نسبة الجوانب متقاربة في أهمية إضافتها في مقترح النظام التشريعي لأنظمة إنترنت الأشياء بالمملكة العربية السعودية.

خلاصة نتائج الدراسة

توصلت الدراسة إلى عددٍ من النتائج، وهي الآتي:

أظهرت نتائج السؤال الأول للدراسة، ومن خلال تحليل محتوى القوانين واللوائح وضوابط إنترنت الأشياء، أن هناك خمسة جوانب رئيسة لأنظمة إنترنت الأشياء، وهي: الخصوصية، والشفافية، والأمان، وجودة البيانات، والبنية التحتية، والتي جرى تحديدها بعد الرجوع للقوانين والسياسات والضوابط التي تختص بإنترنت الأشياء التي أقرتها بعض الدول. وقد استمدت الباحثة مواد هذه الجوانب من القوانين والسياسات والضوابط الآتية:

- قانون حماية الخصوصية الإلكترونية في الاتحاد الأوربي.
- سياسة تشفير البيانات في مدينة نيويورك.
- سياسة تصنيف البيانات في مدينة نيويورك.
- قانون البيانات المفتوحة في مدينة نيويورك.
- ضوابط إنترنت الأشياء في مدينة نيويورك.
- أمان إنترنت الأشياء للمستهلكين في المملكة المتحدة.
- لائحة تنفيذية مرتبطة بشفافية معالجة البيانات الشخصية الواردة في اللائحة العامة لحماية البيانات.
- قانون كاليفورنيا رقم **327**.

أظهر الخبراء المشاركون في الدراسة تباينًا في مدى مناسبة أو عدم مناسبة المواد التي تندرج تحت الجوانب الرئيسة للنظام المقترح في الجولة الأولى من أسلوب دلفاي. وعليه، فقد تم أخذ ملاحظات ومقترحات الخبراء لإعادة إرسال القائمة كجولة ثانية؛ حتى يراجع الخبراء استجاباتهم مرة أخرى في ضوء آراء البقية، وذلك في محاولة لتقريب وجهات النظر بينهم، والتأكيد على أهمية الحاجة إلى تحديد مدى مناسبة كل عبارة (مادة) من العبارات

(المواد) المدرجة تحت الجوانب الخمسة (الخصوصية– الشفافية– الأمان– جودة البيانات– البنية التحتية) والمستندة إلى قوانين ولوائح وضوابط الدول فيما يتعلق بإنترنت الأشياء. وقد تم إعداد قائمة الجولة الثانية وفقًا للآتي:

- الإبقاء على جميع العبارات التي حصلت على إجماع أو شبه إجماع بنسبة تتراوح ما بين 100%–80%.
- إضافة مقترحات الخبراء المتوافقة مع جوانب الاستبانة.

كما أظهرت نتائج الدراسة وجود إجماع وتوافق في الرأي للعبارات التي شملتها الجولة الثانية، وقد بلغت نسبة الاتفاق لكل عبارات الجوانب الرئيسة فوق80%؛ مما يعكس أهمية توفر هذه المواد في النظام التشريعي المقترح لإنترنت الأشياء، وبناءً على نتائج الجولة الأولى والثانية، تم إعداد القائمة الأساسية للجوانب الرئيسة للنظام التشريعي المقترح لأنظمة إنترنت الأشياء في المملكة العربية السعودية، وقد تم ترتيبها وفقًا للنسبة المئوية لكل جانب.

أظهرت نتائج الدراسة أن الخبراء المشاركين قد اتفقوا بنسبة 81% فأكثر على المواد المتعلقة بخصوصية إنترنت الأشياء، عدا المادة التي تنص على أنه (يجب حذف المستخدم عندما يتوقف عن استخدام خدمة ما من خدمات إنترنت الأشياء)، والتي حصلت على اتفاق بنسبة 67%، ولاستناد هذه المادة إلى القاعدة رقم (6) من الضوابط التي وضعتها المملكة المتحدة تحت مسمّى (أمان إنترنت الأشياء للمستهلكين) " Consumer Internet of Things (IoT) Security for manufacturers"، وكذلك المادة رقم (7) من قانون حماية الخصوصية الإلكترونية EU/0003/2017 ، فقد رأت الباحثة وجوب إضافتها في المقترح.

أظهرت نتائج الدراسة أن الخبراء المشاركين قد اتفقوا بنسبة 81% فأكثر على المواد المتعلقة بمتطلب شفافية إنترنت الأشياء؛ فقد جاء هذا الجانب في المرتبة الثالثة في الأهمية بين الجوانب الخمسة الأساسية (الخصوصية– الشفافية– الأمان– جودة البيانات– البنية

التحتية)، وقد استمدت معظم عبارات هذا الجانب إلى الضوابط المتعلقة بالشفافية بموجب اللائحة 679/2016، و ضوابط إنترنت الأشياء بمدينة نيويورك.

أظهرت نتائج الدراسة أن الخبراء قد اتفقوا بنسبة 81% وأكثر على مدى مناسبة إدراج مواد هذا الجانب في المقترح. فقد استندت معظم عبارات هذا الجانب إلى قانون كاليفورنيا رقم SB327، وكذلك ضوابط أمان إنترنت الأشياء للمستهلكين التي وضعتها المملكة المتحدة للحفاظ على أجهزة وبيانات المستخدمين من التهديدات الأمنية.

أظهرت نتائج الدراسة أن الخبراء المشاركين قد اتفقوا بنسبة 81% فأكثر على المواد المتعلقة بجودة بيانات إنترنت الأشياء المفترض تطبيقها على أنظمة إنترنت الأشياء في المملكة العربية السعودية، وقد جاءت العبارة رقم (9) كأعلى العبارات نسبة والتي تنص على ضرورة وجود تأمين يجبر عليه مزوّدي خدمات إنترنت الأشياء ومصنّعي الأجهزة في المملكة العربية السعودية ضدّ الأخطاء المصنعية والهجمات الأمنية والمخاطر البيئية؛ حيث حصلت على إجماع بنسبة 96%، وهي مقترح اقترحه مجموعة من الخبراء المشاركين. و قد استندت معظم عبارات هذا الجانب إلى اللائحة التنفيذية لقانون البيانات المفتوحة في مدينة نيويورك رقم 2012/011.

أظهرت نتائج الدراسة أن الخبراء المشاركين قد اتفقوا بنسبة 81% فأكثر على المواد المتعلقة بمتطلب البنية التحتية لإنترنت الأشياء؛ وقد استندت عبارات هذا الجانب إلى ضوابط البنية التحتية التي طرحتها مدينة نيويورك، والتي أكدت على وجوب التزام الهيئة المسؤولة بقائمة جميع الأصول سواءً العامة أو الخاصة التي يتم تثبيت أجهزة إنترنت الأشياء عليها، كما يجب أن تحتفظ الهيئة بقائمة جرد لكل أجهزة إنترنت الأشياء الموجودة داخل الدولة.

وقد أظهرت الدراسة أن جانب البنية التحتية جاء كأهم جانب بنسبة 92%، يليه جانب أمان إنترنت الأشياء بنسبة 90%، في حين جاء جانبا الشفافية وجودة بيانات إنترنت الأشياء في المرتبة الثالثة بنسبة 89%، وجانب خصوصية إنترنت الأشياء بنسبة 83%؛ كما

أظهرت نتائج الدراسة أن الاختلاف في ترتيب أهمية كل جانب بالنسبة لمجموعة الخبراء المشاركين، يؤكد على أهمية الأخذ بالاختلافات الثقافية والبيئية بين المجتمعات عند النظر لقوانين وتشريعات إنترنت الأشياء على مستوى الدول.

عاشراً: التوصيات

في ضوء النتائج التي توصلت إليها الباحثة، توصي الدراسة بالآتي:

- الاستفادة من النظام المقترح الذي قدمته الدراسة من خلال نتائجها.
- تشجيع الباحثين بإجراء دراسات متعمقة بكل جانب من الجوانب التي تناولتها الدراسة (وهي: الخصوصية– الشفافية – الأمان– جودة البيانات– البنية التحتية)، من الجانب القانوني المعلوماتي.
- أهمية وجود لائحة تنفيذية أو ضوابط تتناسب واستخدام إنترنت الأشياء وخدماتها في القطاع الحكومي والخاص والقطاع الثالث (المؤسسات الخيرية والمجتمع المدني).

النظام التشريعي المقترح لأنظمة إنترنت الأشياء بالمملكة العربية السعودية

تم اعداد هذا المقترح بناءً على نتائج الدراسة ورأي الخبراء والأنظمة العالمية التي تم الاعتماد عليها في إعداد قائمة بالجوانب الأساسية لأنظمة إنترنت الأشياء (الخصوصية– الشفافية – الأمان– جودة البيانات– البنية التحتية)، كما تم ترتيب مواد النظام بحسب نتائج الدراسة.

المادة الأولى:

يُسمّى هذا المقترح بنظام خدمات إنترنت الأشياء.

المادة الثانية:

يقصد بالعبارات الآتية، المعاني المبيّنة أمامها:

- إنترنت الأشياء: شبكة من الأشياء المتصلة بالإنترنت القادرة على جمع وتبادل البيانات فيما بينها.
- الخصوصية: قدرة الفرد على السيطرة على البيانات الشخصية التي يتم جمعها من قبل الأشياء الذكية المحيطة.
- الشفافية: القدرة على فهم البيانات التي تنشئها تطبيقات إنترنت الأشياء وترسلها.
- الأمان: تأمين وحماية أجهزة إنترنت الأشياء والشبكات التي ترتبط بها من الاختراق والوصول إلى البيانات التي يتم نقلها وإساءة استخدامها.
- جودة البيانات: مدى ملائمة البيانات التي تم جمعها من الأشياء الذكية لتوفير خدمات لمستخدمي إنترنت الأشياء.
- البنية التحتية: هي قابلية التوسع والامتداد وقابلية التشغيل المتبادل بين أجهزة إنترنت الأشياء الغير المتجانسة.
- المصادقة: تعني طريقة للتحقق من صلاحية المستخدم أو العملية أو الجهاز للوصول إلى الموارد في نظام المعلومات.

المادة الثالثة:

يهدف هذا النظام إلى تحسين البنية التحتية و معايير وأمن أجهزة إنترنت الأشياء، والحفاظ على خصوصية وشفافية وأمن مستخدمي خدمات إنترنت الأشياء في المملكة العربية السعودية.

المادة الرابعة: وجود خطط مرنة لأنظمة إنترنت الأشياء تضمن استمرارية الخدمة في حال وقوع الكوارث الطبيعية.

المادة الخامسة: الاستفادة من الشبكات السلكية واللاسلكية الموجودة حاليًا كلما كان ذلك ممكنًا و مناسبًا.

المادة السادسة: وجود اتفاقيات واضحة لترخيص الموقع وشروط الخدمة المقررة لكل أجهزة إنترنت الأشياء ومعدّات الشبكات المثبتة من قبل الدولة.

المادة السابعة: تقوم الهيئة الحكومية المسؤولة بنشر معلومات عامة عن أنظمة إنترنت الأشياء.

المادة الثامنة: تحتفظ الهيئة الحكومية المسؤولة بالتفاصيل والمعلومات الخاصة بالشبكات التي تستخدمها أجهزة إنترنت الأشياء.

المادة التاسعة: تحتفظ الهيئة الحكومية المسؤولة بقائمة الأصول العامة أو الخاصة التي يتم تثبيت الأجهزة عليها.

المادة العاشرة: وجود آلية لمراقبة وتحديد نقاط الضعف الأمنية وتصحيحها –داخل أجهزة إنترنت الأشياء– بواسطة مصنّعي هذه الأجهزة.

المادة الحادية عشرة: ضمان عدم تعديل البيانات من قبل جهة خارجية؛ حفاظًا على أمان بيانات المستخدمين.

المادة الثانية عشرة: وضع نظام لتأمين إنترنت الأشياء وحمايتها من مخاطر: القرصنة– أخطاء النظام –العبث – والمخاطر البيئية.

المادة الثالثة عشرة: تحديث مكونات البرامج في الأجهزة المتصلة بإنترنت الأشياء بشكل مستمر.

المادة الرابعة عشرة: يسمح لمقدمي شبكات وخدمات إنترنت الأشياء بمعالجة البيانات التي تم جمعها فقط إذا كان ذلك بغرض الحفاظ على أمن شبكات وخدمات إنترنت الأشياء، أو اكتشاف المخاطر الأمنية.

المادة الخامسة عشرة: يسمح لمقدمي شبكات وخدمات إنترنت الأشياء بمعالجة البيانات التي تم جمعها إذا كان ذلك بغرض الامتثال لالتزام قانوني يخضع له المزوّد في المملكة.

المادة السادسة عشرة: تلتزم أجهزة إنترنت الأشياء وتطبيقاتها وأنظمتها بالشفافية الكاملة حول عمليات جمع البيانات ونقلها ومعالجتها واستخدامها.

المادة السابعة عشرة: يحق للمستخدم دائمًا التحكم في ما يخصه من البيانات الشخصية التي تجمعها الشركات.

المادة الثامنة عشرة: تكون سياسة مزوّد خدمة إنترنت الأشياء صريحة وواضحة، ويسهل فهمها.

المادة التاسعة عشرة: يحق للمستخدم مطالبة الشركات المصنّعة ومقدمي خدمات إنترنت الأشياء بالإفصاح عن كيفية استخدام البيانات الشخصية التي تم جمعها.

المادة العشرون: تعريف مستخدمي أجهزة وخدمات إنترنت الأشياء بالمخاطر والقواعد والضمانات والحقوق المتعلقة بمعالجة بياناتهم الشخصية.

المادة الحادية والعشرون: تكون المعلومات المقدَّمة للمستخدم موجزة وشفافة ومفهومة ويمكن الوصول إليها بسهولة.

المادة الثانية والعشرون: وجود تأمين إجباري على شركات ومقدّمي خدمات إنترنت الأشياء ضدّ الأخطاء الفنية أو المخاطر أو الهجمات.

المادة الثالثة والعشرون: تحديث البيانات التي يتم جمعها عن طريق أجهزة إنترنت الأشياء لتجنب الأخطاء التي قد تسببها معالجة بيانات قديمة.

المادة الرابعة والعشرون: وجود آلية لجودة عمل المستشعرات والأجهزة المرتبطة بإنترنت الأشياء.

المادة الخامسة والعشرون: قيام مقدّمي خدمات إنترنت الأشياء بالتحليل الفوري للبيانات التي تم جمعها؛ لمنع تراكمها.

المادة السادسة والعشرون: وجود آليات تحقق تكامل البيانات التي يتم جمعها عن طريق الأجهزة المرتبطة بأنظمة إنترنت الأشياء.

المادة السابعة والعشرون: تصنيف البيانات والمعلومات الشخصية التي يتم جمعها عن طريق إنترنت الأشياء على أنها بيانات خاصة وسرية.

المادة الثامنة والعشرون: الحصول على "موافقة المستخدم" بشكل صحيح وقانوني قبل الشروع في معالجة بياناته الشخصية مع إتاحة الفرصة له بحذفها في أي وقت.

المادة التاسعة والعشرون: يتم جمع البيانات لأغراض محددة وصريحة، وألا تُعاد معالجتها مرة أخرى بطريقة لا تتوافق مع تلك الأغراض.

المادة الثلاثون: وجود هيئة تراقب تطبيق الأطراف الأخرى لمعايير الخصوصية التي يلتزم بها مزوّد خدمة إنترنت الأشياء نفسه عند مشاركة البيانات داخلياً وخارجياً.

المـراجـع:

أولاً: المراجع العربية

1. خليفة، إيهاب (2012). ***إنترنت الأشياء: تهديدات أمنية متزايدة للأجهزة المتصلة بالإنترنت***. مجلة اتجاهات الأحداث، ع19، ص58.

ثانيًا: المراجع الاجنبية

1. ARTICLE 29 DATA PROTECTION WORKING PARTY. (2016). ***Guidelines on transparency under Regulation 2016/679.*** European Parliament, p 6.
2. Ashton, Kevin (2009, June 22). ***That " Internet of Things" things***. RFID Journal. Retrieved from: www.rfidjournal.com/ article/ print/4986
3. Atzori, Luigi, Ierab, Antonio, Morabitoc, Giacomo. (2010). ***The Internet of Things: A survey***. The International Journal of Computer and Telecommunications Networking, 54 (15), p 3. Retrieved from: 10.1016/ j.
4. Cheng, Y., Naslund, M., Selander, G., Fogelstrom, E. (2012). ***Privacy in machine-to-machine communications A state-of-the-art survey***. IEEE International Conference on Communication Systems (ICCS), p 579.
5. DIRECTIVE (EU) 2016/1148, ***concerning measures for a high common level of security of network and information systems across the Union (2016).*** Official Journal of the European Union, THE EUROPEAN PARLIAMENT AND OF THE COUNCIL. Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN
6. Dorsemaine, B, Gaulier, J, Wary, J, Kheir, N, Urien, P. (2015, September). ***Internet of Things: A Definition & Taxonomy.*** 9th International Conference on Next Generation Mobile Applications, Services and Technologies, UK, Cambridge
7. European Data Protection Board. (2019). ***Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR in particular regarding the competence, tasks and powers of data protection authorities.*** Opinion of the Board (Art. 64), P 3.
8. Federal Trade Commission Staff Report. (2015, January). ***Internet of Things: Privacy & Security in a Connected World***. p 5. Retrieved from: https:// www.ftc.gov/system/files/documents/ reports/federal-trade-commissionstaff-report-november-2013-workshop-entitled-internet-thingsprivacy/150127iotrpt.pdf.

9. Gazis, V. (2017). ***A Survey of Standards for Machine-to-Machine and the Internet of Things***. IEEE Communications Surveys & Tutorials,19(1), par (4).

10. Goodman, Ellen. (2015). ***The Atomic Age of Data: Policies for the Internet of Things***. The Aspen Institute, Communications and Society Program. United States of America: NW, par 8.

11. Goyal, Pandey, Sahai, Waters, 2006, January). ***Attribute-based encryption for fine-grained access control of encrypted data.*** ACM Conference on Computer and Communications Security 2006, p 81,89.

12. ‹Kopet, Hermann. (2011**). *Design Principles for Distributed Applications*.** Real-Time Systems series, Springer Science & Business Media. 2nd ed, p 308.

13. Johnson, Shawn. (2016). ***A Law and Economics Approach to Privacy Policy Misstatements: Considering the Need for a Cost-Benefits Analysis in the FTC's Deception Framework***. Columbia Science and Technology Law Review, 18(1), p 79.

14. Joshi, R.D., Kulkarni, C., Patki, A.B., Wani, P.W. (2016). ***Emerging trends in IoT standards and legislation.*** 2016 International Conference on Internet of Things and Applications (IOTA), p 373-378.

15. Khalil, Jawad. (2019*). **Saudi Arabian Internet of Things Market Forecast*** ‹Riyadh, Saudi ***and Analysis 2018-2022***. International Data Corporation (IDC) Arabia, p 2,12,13.

16. Maxwell, Winston, Zou, Roy, Xie, Jessie, Brennan, Mark, Sura, Arpan. ‹(2019, March 28). ***A comparison of IoT regulatory uncertainty in the EU and the United States***. Hogan Lovells, Washington, DC. ***‹China***

17. D., Papapanagiotou, I., Yang, B. (2017). ***Internet of Things:*** ‹Mendez ***Survey on Security and Privacy***. Information Security Journal, Purdue university, p 13.

18. Okoli, Chitu, Pawlowski, Suzanne. (2004). ***The Delphi method as a research tool: an example, design considerations and application.*** Information and Management, 42(1), p 15-29. doi.org/10.1016/j.im.2003.11.002

19. **João.** (2019). ***Internet of Things: The Global Regulatory*** ‹**Pedro *Ecosystem and the Most Promising Smart Environments Part II.*** The National Law Review. Retrieved from: https://www.natlawreview.com/article/internet-things-global-regulatory-ecosystem-and-most-promising-smart-environments

20. PINTÓ, Carlos. (2018). ***privacy and security for consumers and businesses in the internet of Things (IoT).*** Official Journal of the European Union, p 3.

21. Saint, Martin, Garba, Aminata. (2016, September 2). ***Technology and Policy for the Internet of Things in Africa.*** TPRC 44: The 44th Research Conference on Communication, Information and Internet Policy Journal.

22. ‹ A., Tippenhauer, N., Lee, J., Elovici, Y. (Dec‹Siboni, S., Shabtai 2016). ***Advanced Security Testbed Framework for Wearable IoT Devices***. ACM Trans, Internet Technology, 16(4), p 125.

23. Stone, Peter, Counsel, Carley, Hopkins, Alto, Palo. (2018). ***Government Action on IoT Security***. International Journal of IoT Law and Public Policy, 1), p 26.(London, 1

24. Tabusca, Alexandru, Maria, Silvia, Gabriel, Garais. (2018). ***IoT and EU Law – E-Human Security.***

25. The UK's Department for Digital, Culture, Media and Sport. (2018). ***Code of Practice for Consumer IoT Security***. P 4-5.

26. Tzafestas, Spyros. (2018). ***Ethics and Law in the Internet of Things World***. Smart Cities, 1(1), p 98-120.

27. Walkerm, Mark, Shockey, Kelton, Neiman, Andrew, Stephan, Ashtyn. (2018, September 10). ***Awakening Global Governments: An International Survey of Internet of Things Regulation.*** TPRC 46: The 46th Research Conference on Communication, Information and Internet Policy.

28. Weber, R. (2010). ***Internet of Things – New security and privacy challenges?*** Computer Law & Security Review, 26, p 23-30.