منتدى
حوكمة المعلوماتية
INFORMATICS GOVERNANCE FORUM

التقرير النهائي لمخرجات منتدى حوكمة المعلوماتية

FINAL REPORT ON THE OUTCOMES OF THE INFORMATION GOVERNANCE FORUM

منتدى حوكمة المعلوماتية
INFORMATICS GOVERNANCE FORUM

فهرس المحتويات

تمهيد

منتدى حوكمة المعلوماتية هو فاعلية وطنية تسعى المؤسسة الليبية للتقنية وجمعية الانترنت - ليبيا، لإقامتها بشكل سنوي مع مجموعة من أصحاب المصلحة، وتجمع تحت مظلّتها مختلِف الأطراف المعنية بالتحول الرقمي في ليبيا، بما في ذلك الجهات الحكومية، والقطاع الخاص، والمجتمع المدني، والمؤسسات الأكاديمية، كما بادرت المؤسسة بدعوة واحتضان مجموعة استشارية متعددة الأطراف المجتمعية ليكون جزءًا من هذا الحراك الوطني ويعزز من مشاركة المجتمع في صياغة مستقبل الحوكمة الرقمية.

يهدف المنتدى إلى توفير منصة حوارية وتفاعلية؛ لمناقشة القضايا الراهنة والمستقبلية المتعلقة بالحوكمة الرقمية، ووضع السياسات والتشريعات التي تدعم بيئة رقمية آمنة وشفافة ومستدامة.

يعدّ المنتدى فرصة لتعزيز التعاون بين الشركاء المحليين والدوليين، وتبادل الخبرات والممارسات الفضلى، بما يسهم في دفع عجلة التحول الرقمي في ليبيا، وتمكين المجتمع من الاستفادة القصوى من التقنيات الحديثة بطريقة آمنة ومسؤولة.

مقدمة عامة

أقيم منتدى حوكمة المعلوماتية 2025 يوم السبت 2 أغسطس 2025 بفندق كورنثيا - طرابلس، بتنظيم المؤسسة الليبية للتقنية وعدد من الشركاء، وبحضور أكثر من 150 مشاركًا من الجهات الحكومية، والقطاع الخاص، والقطاع الأكاديمي، ومنظمات المجتمع المدني، بهدف تعزيز الحوار حول واقع الحوكمة الرقمية في ليبيا، وبحث التحديات والحلول، وتطوير السياسات والتشريعات ذات الصلة، مع التركيز على: التحول الرقمي، والأمن السيبراني، والذكاء الاصطناعي.

المساهمون في منتدى حوكمة المعلوماتية

1. **اللجنة التنظيمية للمنتدى:**

- أمين يونس صالح - المشرف العام على المنتدى.
- تسنيم المغربي - منسق المنتدى.

- مصطفى فتيتة - مصمم الوسائط المتعددة.
- هبة غانم - مسؤولة النشر في وسائل التواصل الاجتماعي للمنتدى.
- نورا الشيباني - مدققة لغوية للمنشورات.
- المؤسسة الليبية للتقنية ممول وراعي مالي.
- مجتمع الإنترنت - ليبيا، منظمين.

2. **اللجنة الاستشارية:**

- فراس بيزنطي - منسق اللجنة الاستشارية وممثل عن مجتمع الإنترنت - ليبيا.
- خالد امبارك - عضو مستقل.
- محمد الحولة - عضو مستقل.
- منير العدل - ممثل عن الهيئة العامة للمعلومات، القطاع الحكومي.
- رفيق الجنجان - ممثل عن الهيئة العامة للاتصالات والمعلوماتية، القطاع الحكومي.
- محمد الجداع - ممثل عن الهيئة الوطنية لأمن وسلامة المعلومات، القطاع الحكومي.
- عمران الشائبي - شركة رقمنة، القطاع الخاص.
- أسامة منصور - ممثل عن مبادرة أنير، المجتمع المدني.

3. **كُتّاب الجلسات:**

- آلاء الصغير.
- رتاج سليمان.
- خولة عون.
- آلاء الحداد.

- نورا الشيباني.

4. **الجهات المنفذة لورش المنتدى**

- شركة البركة للتأمين.
- الهيئة العامة للاتصالات والمعلوماتية.
- ديوان المحاسبة الليبي.
- مبادرة أنير.
- الهيئة العامة للمعلومات.
- إدارة مكافحة جرائم تقنية المعلومات - جهاز المباحث الجنائية.
- إدارة البحوث والإحصاء - مصرف ليبيا المركزي.

5. **داعمين المنتدى**

- مركز الاتصال الحكومي.
- شركة العنكبوت الليبي.
- شركة why studio.
- مجتمع الانترنت.
- مجتمع الانترنت - ليبيا.
- شركة الواحة للمعارض.
- الهيئة العامة للمعارض والمؤتمرات.

6. **التدقيق والمراجعة**

- نورا الشيباني - المدقق اللغوي والمراجع النهائي للتقرير.
- أمين صالح - مراجعة فنية.

نظرة عامة على الجلسات وورش العمل

تضمن المنتدى مجموعة من الجلسات الحوارية وورش العمل المتخصصة، التي جمعت ممثلين عن الجهات حكومية، والقطاع الخاص، ومنظمات المجتمع المدني، والمؤسسات الأكاديمية.

تناولت هذه الفاعليات قضايا جوهرية مثل الواقع القانوني لحوكمة المعلوماتية، وحوكمة الذكاء الاصطناعي والتقنيات الناشئة، والأمن السيبراني، والسياسات الوطنية للتحول الرقمي، وإدارة النطاق الوطني (.LY).

قُدّمت ورش عمل تطبيقية لتعزيز قدرات المشاركين في مجالات الأمن السيبراني، والتأمين ضد المخاطر الرقمية، واستخدام منصات الذكاء الاصطناعي، وقد كانت هذه الجلسات والورش فرصة لتبادل الخبرات وبناء توصيات عملية لدعم التحول الرقمي الآمن والمستدام في ليبيا.

الجلسة الحوارية الأولى:

الواقع القانوني لحوكمة المعلوماتية في ليبيا

موضوعات الجلسة

الواقع القانوني لحوكمة المعلوماتية في ليبيا، بما يشمل التشريعات، واللوائح، والسياسات، والإستراتيجيات.

إدارة الجلسة

1. أمين صالح - رئيس المؤسسة الليبية للتقنية.

ضيوف الجلسة

2. طارق المصراتي - مدير الإدارة القانونية بالهيئة العامة للاتصالات.
3. نرمين السعدني - نائب رئيس للشرق الأوسط - جمعية الانترنت الدولية.
4. د. محمد الجداع - الهيئة الوطنية لأمن وسلامة المعلومات.
5. أمجد بدر الشويهدي - لجنة الأمم المتحدة للاقتصاد في إفريقيا.

موضوعات النقاش

6. قانون الاتصالات والمعلوماتية رقم 22 لسنة 2010م، الذي لم يُحدّث منذ أكثر من عشر سنوات، والحاجة الملحة لتطويره لمواكبة التطورات التقنية.
7. القانون رقم 8 لسنة 1990م بشأن الاتصالات السلكية واللاسلكية.
8. القرار رقم 985 لسنة 2022م بشأن اللوائح التنفيذية للقانون رقم 22 لسنة 2010م، الذي ضم 11 لائحة لتنظيم قطاع الاتصالات.
9. تشكيل لجنة في 2022م لصياغة مسودة قانون جديد للاتصالات والمعلوماتية، بهدف تعزيز الاستثمار والمنافسة، وتحسين الأداء في القطاعين العام والخاص.

التوصيات

10. الإسراع إلى تحديث الإطار القانوني للاتصالات والمعلوماتية.
11. تعزيز التعاون بين الجهات التشريعية والتنظيمية؛ لضمان مواءمة القوانين للمعايير الدولية.
12. توفير بيئة قانونية داعمة لجذب الاستثمارات وتحفيز الابتكار.

ما نوقش في الجلسة الحوارية

قانون الاتصالات والمعلوماتية

تعمل ليبيا منذ سنة 2010م على قانون رقم 22 لسنة 2010م الذي يهدف إلى تنظيم الاتصالات، وقد وضعه خبراء ومختصون. استمر العمل بهذا القانون، لكننا اليوم في 2025م، وقانون الاتصالات والمعلوماتية لم يُحدّث منذ أكثر من 10 سنوات، والقوانين تحتاج إلى تطوير وتحديث باستمرار.

من القوانين الصادرة في هذا الخصوص القانون رقم 8 لسنة 1990م بشأن الاتصالات السلكية واللاسلكية، ثم إن مجلس الوزراء الليبي أصدر القرار رقم 985 لسنة 2022م بإصدار اللوائح التنفيذية للقانون رقم 22 لسنة 2010م بشأن الاتصالات، بهدف تنظيم قطاع الاتصالات في ليبيا عن طريق تحديد الإجراءات والمتطلبات اللازمة للحصول على التراخيص في هذا القطاع، وقد ضم القرار في جعبته 11 لائحة تنفيذية لتنظيم قطاع الاتصالات.

وفي سنة 2022م أصدر رئيس الهيئة العامة للاتصالات والمعلوماتية قرارًا بتشكيل لجنة لوضع مسودة قانون الاتصالات والمعلوماتية، من أجل وضع إطار تنظيمي للاستثمار والمنافسة والنمو في قطاع الاتصالات والمعلوماتية، وهو إلى ذلك يسعى لرفع مستوى الأداء بقطاع الاتصالات وتقنية المعلومات بشقية العام والخاص، وتحسين فرص الانتقال إلى الاقتصاد الرقمي والمعاملات الإلكترونية.

عملت اللجنة مدة عامين حتى وصلت إلى المسودة النهائية للقانون، وقد شاركت الهيئة مسودة القانون على موقعها الرسمي.

حماية البيانات الشخصية

إن حماية البيانات الشخصية من حقوق الإنسان الأساسية التي تدعمها جميع الدول، وأكثر من 160 دولة لديها قوانين خاصة تعنى بحماية البيانات الشخصية، وتنظم عملية تجميع البيانات ومعالجتها، بدءًا من اتفاقية مجلس أوروبا سنة 1982م بشأن الجرائم الإلكترونية التي تعرف باسم اتفاقية بودابست، حتى مشروع اتفاقية الجزائر بشأن حماية البيانات الشخصية، أما الدول العربية فإن 16 دولة منها بها قوانين لحماية البيانات الشخصية، والدفاع عن حقوق أصحابها، وتجريم تجميع البيانات ومعالجتها من دون إذن أصحابها.

وفي إطار الدولة الليبية، فإن دور الهيئة الوطنية لأمن وسلامة المعلومات في حماية البيانات الشخصية، يتمثل في المشروع الوطني لحماية البيانات الشخصية بمبادة من المجلس الوطني للحريات وحقوق الإنسان، ويجري العمل على صياغة قانون حماية البيانات الشخصية، ووضع هيكلية لمؤسسة تعنى بهذا الشأن، وهذا القانون في مراحله النهائية.

أما فيما يخص اللائحة التنظيمية لحماية البيانات الشخصية ذات الطابع المالي، فإن غياب تنظيم قانوني واضح في ليبيا أو غياب التشريعات أدى إلى تدخل مصرف ليبيا المركزي للإشراف ومتابعة العملية، وقد أُعدت لائحة موفّقة جمعت كل المعايير الدولية الخاصة بحماية البيانات الشخصية، مع بعض المآخذ التي تتطلب تحقيقًا مستمرًّا لضمان فاعليتها.

المجتمع المدني وقانون الجرائم الإلكترونية

يتعلق قانون الجرائم الإلكترونية والتحديات المرتبطة به بتوجيهات المجتمع المدني حول ضرورة حماية المستخدمين والقطاعات المعنية، بأن تكون القوانين أكثر تمكينًا وتتجاوز الجانب الكلاسيكي التنظيمي.

في القوانين الحالية عيوب فنية تعد جزءًا من الهيكل التنظيمي للقطاع، ولذلك فمن المهم وضع تنظيم شامل يضمن الاستفادة من قوانين الخصوصية وسلامة المعلومات، سواء للمستخدم الفردي أو القطاع الخاص، ويعزز فاعلية الحماية والأمن السيبراني.

من خلال التعاون بين المجتمع المدني والقطاع الحكومي والخاص، يمكن تعزيز فعالية قانون الجرائم الإلكترونية وضمان تطبيقه بشكل يراعي خصوصية وأمان المستخدمين، مما يفتح الطريق نحو بيئة رقمية أكثر أمانًا وثقة في ليبيا.

إن المجتمع المدني جزء من المنظومة التقنية في ليبيا، وله دور مهم في وضع التشريعات المتعلقة بالجرائم الإلكترونية، لضمان المصلحة العليا للجميع، وتمكين المستخدم من الاستفادة من التقنية بأمان، وتنظيم القطاع، وقد عمل المجتمع المدني على تقديم توصيات مستمرة للجهات التشريعية، داعيًا إلى صياغة قانون جرائم إلكترونية يتجاوز مجرد الردع القانوني ليشمل آليات حماية حقيقية للمستخدمين، وتوفير تعليم وتوعية حول الأمن الرقمي، إضافة إلى دعم البنية التحتية التقنية اللازمة.

ومع ذلك، يواجه المجتمع المدني تحديات كبيرة في هذا المجال، منها ضعف الموارد، وعدم وضوح أدوار الجهات الحكومية، فضلًا عن التحديات المتعلقة بحماية الخصوصية في ظل غياب بيئة قانونية متكاملة. إن ضعف التوعية المجتمعية يجعل من الضروري أن تنظم هذه منظمات المجتمع المدني برامج تدريبية مكثفة؛ لتعزيز فهم الأفراد والمؤسسات لأهمية الأمن السيبراني وحقوقهم الرقمية.

تحديات تكوين السياسات واللوائح في المنطقة العربية

إن من أبرز الصعوبات في تكوين السياسات واللوائح في المنطقة العربية وجود بعض التحديات مثل التخوف والقلق من وجود المجتمع المدني والقطاع التقني جنبًا إلى جنب مع الحكومات، مما يعرقل عملية تطوير السياسات بفاعلية، ثم إن مدى اقتناع الدور العربي في هذا المجال يختلف من دولة إلى أخرى ويواجه بعض التحفظات. على مدار السنين، وبعد مرور نحو 20 سنة على إنشاء حوكمة الإنترنت، شهدت المنطقة العربية تضاربًا في الأفكار والرؤى حول أهمية هذه السياسات، وهو ما لا يعني بالضرورة الوصول إلى أفق مثالي، لكنه يسلط الضوء على الحاجة لمزيد من الحوار والتفاهم لتحقيق تقدم فعلي.

قوانين الجرائم الإلكترونية

وجهت العديد من الانتقادات الحادة إلى قوانين الجرائم الإلكترونية والتشريعات ذات الصلة. يُذكر أن القوانين وضعية من صنع البشر وتحتاج إلى تطبيق عملي واقعي يكشف عن الثغرات الموجودة فيها، لا سيما في مجالات السلطة التشريعية والتنفيذية، وتعد قوانين الأمر السيبراني ذات خصوصية عالية، ويجب أن تحقق توازنًا دقيقًا بين البعد الأمني وحقوق أصحاب المصلحة، لضمان حماية البيانات وخصوصية الأفراد.

من المهم جدًّا وجود منظومة قانونية متكاملة، فكل دول المجاورة لليبيا تمتلك مؤسسات معنية بحماية البيانات الشخصية والبنية التحتية للتمثيل الرقمي لهوية الفرد، وهو ما يُعد المفتاح العام لعملية المصادقة الإلكترونية. يفرض الواقع القانوني ضرورة التطور المستمر للتشريعات لمواكبة التحولات الرقمية، مع تدخل السلطة أحيانًا لتعديل القوانين، فإن النقطة الجوهرية التي ما زالت بحاجة إلى معالجة هي عدم تحديد مسؤولية الشخص الاعتباري فيما يخص الامتثال للسياسات والقوانين والمعايير.

من المطالب الملحة أيضًا إصدار قوانين خاصة بالذكاء الاصطناعي، وحماية الأطفال، وتنظيم التجارة الإلكترونية. وفي الحالة الليبية، يُشير الواقع إلى أن المرحلة الانتقالية الحالية لا تكفي لتوفير بيئة رقمية آمنة، حتى مع ارتباط ليبيا باتفاقيات دولية تهدف إلى منع التهديدات الخارجية، وهو ما يمتد أثره إلى الداخل.

والسؤال الأهم هو: هل تمتلك الدولة الليبية القدرة اللازمة لمواجهة هذه التحديات وتفعيل هذه الالتزامات؟

دور الهيئة الوطنية لأمن وسلامة المعلومات

تتولى الهيئة الوطنية لأمن وسلامة المعلومات دورًا حيويًّا لكونها مصدر خبرة رئيسي في المجال، فهي تعمل على تقديم الأدلة والتوجيهات الفنية اللازمة لضمان تنفيذ القوانين المتعلقة بالأمن السيبراني وحماية البيانات بفاعلية. إن الهيئة الوطنية لأمن وسلامة المعلومات جهة داعمة تسهم في تطوير المعايير الفنية والإشراف على تطبيقها، مما يعزز من قدرة الدولة على مواجهة التحديات الرقمية وضمان بيئة رقمية آمنة ومستدامة.

مستقبل اللوائح والسياسات في المنطقة العربية

يتوقع أن يشهد مستقبل اللوائح والسياسات في المنطقة العربية تطورًا كبيرًا، لا سيما في السنوات الثلاثة القادمة. يهدف هذا التطور إلى تعزيز البيئة الرقمية، وتنظيم الفضاء الإلكتروني تنظيمًا أكثر فاعلية، ومن المتوقع إصدار سياسات جديدة تلائم التغيرات التقنية، مع التركيز على التنسيق مع الحضور وأصحاب المصلحة، بما يشمل كلا من: المجتمع المدني والقطاع الخاص والحكومات.

أما فيما يخص المجتمع المدني، فإن اللوائح المرتبطة بإصدار قانون الاتصالات والمعلوماتية الجديد ستكون ذات أهمية كبيرة، إذ ستعمل على تنظيم حقوق المستخدمين، حماية البيانات، وضمان الشفافية. أما على مستوى اللوائح، فمن المتوقع تنظيم الطيف الترددي، وتفعيل الرقابة على مقدمي الخدمة، إضافة إلى تنظيم الخدمات البريدية لضمان الجودة والأمان. وفي رأس الهرم، يظل الدستور الليبي هو الأساس، فهو المرجع الرئيسي، وبتضمين القوانين ذات العلاقة في الدستور يمكن ضمان حماية الحقوق والحريات بصورة دائمة، ما يعزز شرعية القانون وسيادته، ويؤسس لبيئة تشريعية قوية تدعم التحول الرقمي والتنمية المستدامة.

دور المجتمع المدني

تواجه ليبيا تحديًا رئيسيًّا يتمثل في ضعف مشاركة المجتمع المدني والمجتمع الأكاديمي، حتى مع أهمية دورهما وكونهما أدوات فعالة لملء الفجوات وتحقيق التنمية الشاملة، فإن الوعي بهذا الدور ما زال محدودًا، وهو ما يُعزى إلى نقص الوعي الكافي لدى الجهات ذات العلاقة حول القيمة التي يمكن أن يضيفها المجتمع المدني، خاصة في سياق دولة حديثة تمر بمرحلة انتقالية، يكون للجميع فيها دور حيويّ في بناء المستقبل.

لذلك، من الضروري أن تتبنى الجهات الحكومية رؤية واضحة ومحددة تُمكن باقي الجهات من مواكبتها ومتابعتها، مع تفعيل المشاركة في جلسات وورش عمل مماثلة لتعزيز التعاون والتواصل. بناء الثقة بين جميع الأطراف هو أساس لتحقيق الأهداف المشتركة، لا سيما في مجال حماية المستخدمين، وهو ما يتطلب تضافر الجهود والتنسيق المستمر.

على الدول أن تحسب التكلفة التي تتكبدها والخسائر الناتجة عن ضعف التنسيق أو نقص التعاون بين الأطراف، فهي مما يؤثر على الاستثمار في البنية التحتية الرقمية، والأمان السيبراني، والتنمية الاقتصادية بصورة عامة، وعليها أن تعلم أن الاستثمار في توعية المجتمع المدني وتفعيل دوره هو استثمار حيوي لضمان استدامة التطور والتحول الرقمي في ليبيا.

توصيات الجلسة الحوارية

1. تحديث قانون الاتصالات والمعلوماتية دوريًّا لمواكبة التطورات التقنية والاحتياجات الحالية، مع ضمان مرونته ليواكب سرعة الأحداث والتقنيات الجديدة.

2. إصدار قوانين واضحة لحماية البيانات الشخصية توافق المعايير الدولية، مع تخصيص مؤسسات رقابية فعّالة تضمن تنفيذها وحماية الخصوصية.

3. وضع إطار تشريعي شامل يعالج جرائم الإنترنت يوازن بين الأمن وحقوق المستخدمين، عن طريق تبني نماذج قوانين عالمية وتجارب ناجحة، مع تكييفها وفقًا للخصوصية الليبية والسيادة الرقمية.

4. تفعيل التعاون بين الجهات التشريعية والتنفيذية لضمان تطبيق السياسات على نحو فعّال، مع إيجاد آليات واضحة للتعاون وعدم تداخل الصلاحيات بين الأطراف المختلفة.

5. تضمين الحقوق والحرية الرقمية في الدستور الليبي لضمان حماية دائمة لحقوق الأفراد الرقمية، مع النظر إلى البعد الإستراتيجي والدسترة على أنها خطوة أساسية.

6. تعزيز مشاركة المجتمع المدني والأكاديمي في وضع السياسات واللوائح لتحقيق التوازن والشمولية، مع إشراك أكبر قدر ممكن من المختصين والمجتمع المدني منذ البداية؛ لضمان ملاءمة القوانين وفاعليتها.

7. بناء الثقة بين جميع الأطراف بواسطة الشراكة والتواصل المستمر، والاعتراف بأهمية الدبلوماسية في عرض الأفكار وتوضيح الاختلافات على المستويين الوطني والإقليمي، إذ إن الرؤى قد تختلف، ولكن الأهداف مشتركة.

8. إنشاء منصات حوار وتعاون مستمرة لتعزيز التفاهم بين القطاعين الحكومي والخاص والمجتمع المدني، ورفع درجة الوعي حول الحقوق الرقمية.

9. تنسيق الجهود العربية والدولية لا سيما في مجالات الأمن السيبراني والسيادة الرقمية، عن طريق الاستفادة من الاتفاقيات والخبرات الدولية، وإنشاء آليات تعاون بين الجهات الفنية والتشريعية لضمان توافق القوانين مع المعايير التقنية.

10. تطوير قدرات الكوادر الوطنية بواسطة برامج تدريبية وورش عمل متخصصة تجمع بين القانون والتقنية، مع إطلاق دبلومات متخصصة لتعزيز التفاهم بين القانونيين والفنيين، فبناء القدرات نقطة فيصلية لمواكبة التطور التقني.

11. إعادة هيكلة القطاع الاتصالات ماليًّا وإداريًّا لضمان المساواة والعدالة، والحفاظ على القدرات الوطنية ومنع هجرة الكفاءات.

12. الاستعداد المسبق بإعداد خطة طوارئ وطنية للتعامل مع الكوارث الطبيعية والأزمات السيبرانية، ما يعزز الاستجابة السريعة والفعّالة في الحالات الطارئة.

13. الحفاظ على التمثيل المتوازن في صنع القرارات الخاصة بالتقنية، وإشراك المجتمع المدني والمختصين والأكاديميين في كل مراحل صياغة القوانين؛ لضمان أن تكون القرارات متزنة وشاملة لكل المعنيين، ولتحقيق الشفافية والفاعلية.

14. تعزيز السيادة الرقمية لحماية بيانات الشعب الليبي وخصوصيته، وذلك بواسطة قوانين نموذجية مستمدة من القوانين العالمية.

15. رفع مستوى الوعي المجتمعي حول أهمية التقنية وحقوق الأفراد الرقمية، عن طريق المنتديات والأحداث والأنشطة التقنية، التي تهدف إلى دفع الدولة لإصدار سياسات وتشريعات تحمي هذه الحقوق.

الجلسة الحوارية الثانية:

حوكمة الذكاء الاصطناعي والتقنيات الناشئة

موضوع الجلسة

كانت الجلسة الثانية من المنتدى بعنوان/ حوكمة الذكاء الاصطناعي والتقنيات الناشئة، وتتضمن كل من:

- الإستراتيجيات العربية الموحدة للذكاء الاصطناعي.
- الميثاق العربي لأخلاقيات الذكاء الاصطناعي.
- خارطة الطريق للبرنامج الوطني للذكاء الاصطناعي والتحول الرقمي.

إدارة الجلسة

- حامد الهوني

ضيوف الجلسة

- عبد القادر الزليتني - الهيئة العامة للاتصالات والمعلوماتية
- إبراهيم جبارة - المؤسسة الليبية للتقنية
- محمد شلابي - الهيئة الوطنية لأمن وسلامة المعلومات

ما جرت مناقشته في الجلسة الحوارية

مبادرات الهيئة الوطنية لأمن وسلامة المعلومات في مجال الذكاء الاصطناعي

الهيئة العامة للاتصالات والمعلوماتية الليبية أعلنت في 17 مايو 2024 عن إطلاق السياسة الوطنية للذكاء الاصطناعي، بالتزامن مع يوم الاتصالات والمجتمع المعلوماتي. تهدف هذه السياسة إلى اعتماد الذكاء الاصطناعي في قطاعات الدولة المختلفة على نحو مسؤول وأخلاقي.

أبرز نقاط السياسة هي وضع أُطر أخلاقية ومعايير شفافية وعدالة وحماية البيانات، وتحفيز الاستثمار في البحث والتطوير والابتكار في هذا المجال، وبناء البنية التحتية الرقمية اللازمة، مثل

شبكات إنترنت سريعة والبيانات الحكومية المفتوحة، وتنمية القدرات بدمج الذكاء الاصطناعي في المناهج التعليمية وبرامج التدريب الوطنية.

وفي أغسطس 2023م، تأسست لجنة الذكاء الاصطناعي تحت وزارة الاقتصاد والتجارة في طرابلس، لتعمل على تطوير نماذج استخدام الذكاء الاصطناعي؛ لتحسين الأداء الاقتصادي المؤسسي، وتعزيز التعاون بين القطاعات التقنية الحكومية والخاصة.

لقد شاركت ليبيا في الاجتماع الثامن لفريق العمل العربي للذكاء الاصطناعي في القاهرة (27-28 نوفمبر 2024م)، فساهمت في صياغة الرؤية الإستراتيجية العربية المشتركة، وشاركت في الورشة الخاصة بمشروع ميثاق أخلاقيات الذكاء الاصطناعي العربي أيضًا.

أصدرت الهيئة قرارات تنظيمية عدة في 2024م؛ بهدف تنظيم نشاطات خدمات الأمن السيبراني، ومع أن هذه القرارات لا ترتبط مباشرة بالذكاء الاصطناعي، فإنها تؤسس لإطار تنظيمي محكم يُهيئ بيئة مناسبة لاعتماد حلول الذكاء الاصطناعي في خدمات الأمن السيبراني. حتى مع هذا التقدم، لا تزال ليبيا في مراحلها الأولى من تطوير التشريعات المتخصصة في الذكاء الاصطناعي، مع غياب هيئة مستقلة لحماية البيانات أو قانون حماية بيانات شامل إلى الآن.

مساهمة المؤسسة الليبية للتقنية في مجال الذكاء الاصطناعي

المؤسسة الليبية للتقنية هي جزء من البرنامج الوطني الليبي للذكاء الاصطناعي، وهي تولي اهتمامًا كبيرًا لتعزيز الاستخدام الأخلاقي والمسؤول للتقنية في المجتمع. يستند الميثاق الخاص بالبرنامج الوطني الليبي للذكاء الاصطناعي إلى المبادئ والتوصيات الموجهة من الميثاق العربي المبني على معايير اليونيسكو، وقد وضع الميثاق إطارًا واضحًا لضمان الاستخدام الأمثل للتقنية، بما يخدم مصلحة المستخدم الليبي، وبما يجنب سوء الاستخدام والانحرافات الأخلاقية. في نفس الوقت، يسعى العالم إلى توجيه الاستخدام المدني والأخلاقي للتقنية عامة، والذكاء الاصطناعي على نحو خاص، وتنظيمه للحفاظ على القيم الإنسانية، وضمان استدامة التطور التقني بطريقة واعية ومسؤولة.

حوكمة الذكاء الاصطناعي

لكل دولة ظروفها ومتطلباتها التي يجب أن تؤخذ في الاعتبار عند صياغة ميثاق استعمال الذكاء الاصطناعي، وفي نفس الوقت يكون الميثاق قائمًا على المبادئ العامة التي تحددها المنظمات الدولية، فيما توضع حدود عريضة على مستوى العالم كله لتنظيم الاستخدام المسؤول للذكاء الاصطناعي على مستوى العالم. إن هذا التوازن بين التنظيم المحلي والعالمي ضروري؛ لضمان حماية الحقوق، وتحقيق الفوائد المرجوة من تقنيات الذكاء الاصطناعي على نحو مسؤول، وبالتنسيق مع كل الأطراف المعنية.

دور الهيئة الوطنية لأمن وسلامة المعلومات في حوكة الذكاء الاصطناعي

يفرض الوضع الحالي وضع سياسات تنظم هذا الشأن، والهيئة تقدم جهودًا متميزة في تطوير مجال الذكاء الاصطناعي وتنظيمه، بفرض سياسات واضحة تنظم هذا القطاع وتوجه استخدامه. وفي إطار هذه الجهود، أعلنت الهيئة مؤخرًا عن إطلاق أول مساعد ذكاء اصطناعي خاص بها، سُمّي (نيسا AI)، وهو يوافق الإستراتيجية الوطنية لأمن وسلامة المعلومات.

يُعد هذا النموذج (نيسا AI) تطبيقًا محليًّا يساعد في الإجابة عن الاستفسارات عن الإستراتيجيات والسياسات الوطنية المتعلقة بالأمن السيبراني، على سبيل المثال: يمكن للزوار من خارج طرابلس الاستفسار عن المعايير المطبقة في بيئة العمل داخل الهيئة الوطنية لأمن وسلامة المعلومات، ومقارنة ذلك بما هو موجود في مدنهم ومؤسساتهم، ما يعد نقلة نوعية في تقديم هذه الخدمات. والأهم أن أي شخص يمكنه إنشاء حساب وتجربة هذا النموذج بسهولة، مع إمكانية تلقي مقترحات وتوصيات لتحسين (نيسا AI)، ما يعزز من تفاعل المجتمع مع مبادرات الهيئة.

ما يميز نموذج الذكاء الاصطناعي (نيسا AI) عن النماذج المفتوحة الأخرى هو أنه مدرب على قاعدة المعرفة الخاصة بالهيئة فقط، ولا يمنح معلومات خارجية، لذا فهو يضمن دقة عالية في الإجابات، ويقدم تفاصيل دقيقة تتعلق بالسياسات والمعايير الداخلية، ما يجعله أداة فعّالة في دعم الأمن السيبراني وتعزيز الوعي والمعرفة داخل الهيئة وخارجها.

رحلة تطوير أداء نموذج الذكاء الاصطناعي (نيسا AI)

شهدت رحلة تطوير أداء نموذج الذكاء الاصطناعي (نيسا AI) الكثير من الخطوات المهمة. بدأت الهيئة باستخدام نماذج مفتوحة المصدر بدلًا من بناء النموذج من الصفر، فاستعان

المطورون بنماذج مفتوحة المصدر بما يناسب احتياجات العمل. من بين النماذج المختارة كان نموذج قيما 3 من جوجل، وذلك لأنه نموذج استدلالي يُجري عملية التفكير ويبحث ويدقق قبل أن يقدم الإجابة، مما يضمن دقة المعلومات التي يوفرها.

أما فيما يخص مصدر البيانات، فقد حوّل المطورون البيانات إلى ملفات يمكن للجهاز قراءتها بسهولة، للمساعدة في عملية التدريب. استمرت مرحلة التدريب مدة أربعة أشهر تقريبًا. النموذج في مرحلة الإطلاق الآن، وهو متاح حاليًّا ليجربه الجمهور، وليتمكن المستخدمون من الاستفادة من قدراته.

لا تتوفر إستراتيجية واضحة لاستعمال الذكاء الاصطناعي في القطاع العام في ليبيا في الوقت الحالي، وإذا كانت موجودة، فستعمل الهيئة على تطبيقها، علمًا بأن معظم الشركات والمؤسسات حول العالم بدأت بالفعل في تطبيق مساعدات الذكاء الاصطناعي؛ لتحسين عملياتها وتعزيز كفاءتها.

من الفوائد المهمة لاستخدام تقنيات الذكاء الاصطناعي حماية البيانات الداخلية، فالذكاء الاصطناعي يعزز الأمان ويحافظ على المعلومات الحساسة، ثم إن استخدام الذكاء الاصطناعي المحلي في المؤسسات المحلية يساعد على الحفاظ على البيانات من التسريب، ويحدّ من الاعتماد على أنظمة خارجية قد تكون أكثر عرضة للمخاطر الأمنية والهجمات السيبرانية.

أوجه الاختلاف بين الإستراتيجية العربية الموحدة والإستراتيجيات المحلية

لا تعارض بين الإستراتيجية العربية الموحدة والإستراتيجيات المحلية فيما يخص تنظيم استخدام الذكاء الاصطناعي. الإستراتيجية العربية الموحدة قيد الإعداد حاليًّا بعد عقد ورش عمل وإعداد أوراق علمية تدعمها. أمّا ميثاق أخلاقيات الذكاء الاصطناعي فهو يتبع نفس النهج، مع مراعاة الواقع الديني والثقافي والاجتماعي في ليبيا عند تطبيق التجارب العالمية فيها.

إضافة إلى ذلك، تسعى كل دولة لإعداد إستراتيجيتها الخاصة، على غرار الإستراتيجية العربية، لتناسب ظروفها واحتياجاتها المحلية. ويُعد تنظيم استخدام أدوات الذكاء الاصطناعي من الأمور المهمة التي تتطلب وضع إطار قانوني واضح. وفي هذا السياق، يجري العمل حاليًّا على تطبيق الإستراتيجية الموضوعة، مع وضع عقوبات مناسبة للمتجاوزين. ومع أن الميثاق يتضمن

توجيهات عامة، فإن طريقة التنفيذ والالتزام بها يعتمد على كل دولة على حدة، وفق ظروفها واحتياجاتها المحلية.

لقد وضع الاتحاد الأوروبي قانونًا رادعًا في عام 2023م، وهو الجهة الوحيدة التي أطلقت قوانين صارمة حتى الآن، وقد صنف الأخطاء المرتبطة باستخدام الذكاء الاصطناعي إلى أربعة أخطار رئيسية. ومع ذلك، ما زالت الحاجة ملحة إلى صياغة لائحة حقيقية وفعّالة تجرم المخالفين وتضع آليات واضحة للمحاسبة، إذ ليس من رادع قانوني أو لوائح تفرض العقوبات على المستخدمين المخالفين حتى هذه اللحظة.

وفيما يخص المصادر التي تستخدم الذكاء الاصطناعي، فقد حدد الاتحاد الأوروبي الجهات المعنية، وهي المطورون والمستخدمون. تشير البيانات إلى أن 13% من الهجمات السيبرانية الأخيرة كانت مصدرها تقنية الذكاء الاصطناعي، ما يسلط الضوء على أهمية تنظيم استخدامها تنظيمًا صارمًا. من ناحية أخرى، نجحت المؤسسات التي تعتمد على الذكاء الاصطناعي في تحسين أدائها بنسبة تصل إلى 9%، ما يدل على الفوائد الكبيرة التي يمكن تحقيقها عند الاستخدام المسؤول والمنظم لهذه التقنيات.

تراخيص استخدام الذكاء الاصطناعي

من الضروري وضع إطار قانوني شامل ينظم عمل الذكاء الاصطناعي في ليبيا، بالتعاون مع الدول العربية والمنظمات الدولية، بهدف حماية المجتمع من التبعيات المحتملة لهذه التقنية. يتطلب ذلك إعداد قانون خاص بالذكاء الاصطناعي يتضمن حماية البيانات، وحقوق الملكية الفكرية، وأطر الأمان، إضافة إلى نظام تراخيص واضح يحدد الشروط والمتطلبات لاستخدام التقنيات أو تطويرها، لضمان الالتزام بالمعايير الدولية والمحلية. إن التعاون والشراكة مع جميع أصحاب المصلحة، بما في ذلك الحكومة، والقطاع الخاص، والمجتمع المدني، والجامعات، ضروري لضمان أن يكون العمل منسقًا وواقعيًا، ويخدم الأهداف الوطنية بطريقة سليمة.

تصور المجتمع المدني للذكاء الاصطناعي

يتمثل تصور المجتمع المدني للذكاء الاصطناعي في وضع إطار تنظيمي وتراخيص معينة لضمان استخدامه استخدامًا آمنًا ومسؤولًا، إذ يعد المجتمع أن الذكاء الاصطناعي أكثر تعقيدًا من الأمن السيبراني وأكثر حساسية، ما يتطلب اهتمامًا خاصًا واحتياطات إضافية.

يلاحظ أن بعض أنظمة الذكاء الاصطناعي تعمل في أماكن معينة دون علم أصحاب القرار، ما يثير مخاوف بشأن الشفافية والسيطرة. ومن ثم لا يمكن البدء بأي نشاط مرتبط بالذكاء الاصطناعي إلا تحت الرقابة المباشرة وتحت أنظار القانونيين؛ لضمان الالتزام بالأطر الأخلاقية والقانونية، وحماية حقوق المستخدمين والمصالح العامة.

التطور التقني والتطور القانوني

تتطور التقنية بسرعة كبيرة، وغالبًا ما يكون القانون غير مواكبًا لهذه التطورات، ما ينتج فجوات تنظيمية ومخاطر محتملة. الغرض من الحوكمة والسياسات والتشريعات هو تقليل هذه المخاطر وضمان الاستخدام المسؤول للتقنية، لا سيما مع تطور الذكاء الاصطناعي.

أما فيما يخص استعمال الذكاء الاصطناعي لأغراض أكاديمية أو بحثية، فأحد المقترحات أن يكون ذلك عن طريق منصة إلكترونية تسهل عملية الترخيص، بهدف تسريع الإجراءات وعدم تقييد الطلاب والأكاديميين بالبيروقراطية كما يُعامل أصحاب الأعمال والشركات، مع الحفاظ على المعايير والضوابط اللازمة. المهم في كل ذلك هو ضمان الأمان، والتحقق من أن استخدام الذكاء الاصطناعي يكون في المجال المناسب، وأن يكون منظمًا وموثوقًا، ويخدم الأهداف على نحو مسؤول ومتزن.

حوكمة الذكاء الاصطناعي في ليبيا

إنّ وجود حظر على استعمال بعض التقنيات في ليبيا يمثل تحديًا، لكن لا يجعل الاستفادة من تقنيات الذكاء الاصطناعي مستحيلًا. يمكن العمل على تجاوز ذلك بواسطة إستراتيجيات متعددة، منها:

- **تحديث القوانين والسياسات:** كما حدث سابقًا مع حظر بعض التقنيات، يمكن إصدار قوانين مرنة تسمح باستيراد التقنيات الضرورية أو تطويرها، مع وضع ضوابط صارمة لضمان الامتثال والمعايير.
- **إنشاء منصات تواصل مع المصنّعين:** بأن تتواصل الهيئة المختصة مع المنتجين والمصنعين الدوليين عن طريق جهة تنسيقية، لتسهيل استيراد التقنيات أو تطوير بدائل محلية.

- **دور المجتمع المدني:** للمجتمع المدني دور مهم في فتح مجال استيراد المعدات والأدوات اللازمة، بإنشاء مؤسسات أو منظمات معترف بها، تعمل على دعم صناعة الذكاء الاصطناعي محليًّا، وتوفير أدوات وتقنيات بديلة.
- **السياسات المستقبلية:** من المتوقع أن تتطور السياسات الإستراتيجيات في ليبيا، مثل ما حدث في الإمارات من إنشاء هيئات خاصة بالذكاء الاصطناعي، لضبط عمليات الاستيراد والرقابة على التقنية.
- **العمل ضمن إطار دولي:** يمكن الاعتماد على التعاون مع منظمات دولية أو اتفاقيات تسهّل وصول التقنيات بطريقة قانونية وآمنة، مع الالتزام بالمعايير الدولية.

باختصار يمكن بناء منظومة مرنة ومتطورة حتى مع الحظر، عن طريق التعاون بين المؤسسات والمجتمع المدني والدعم الحكومي، لخلق بيئة مناسبة لاستيراد تقنيات الذكاء الاصطناعي وتطويرها في ليبيا.

توصيات الجلسة الحوارية

1. صياغة قانون وطني شامل للذكاء الاصطناعي يشمل حماية البيانات الشخصية، وحقوق الملكية الفكرية، وأطر الأمان، مع نظام تراخيص واضح لاستخدام وتطوير التقنيات.
2. وضع لوائح تنظيمية للعقوبات على الاستخدام غير المسؤول أو غير الأخلاقي لتقنيات الذكاء الاصطناعي، لضمان الالتزام بالمعايير الأخلاقية والقانونية.
3. إنشاء هيئة وطنية مستقلة مختصة بحوكمة الذكاء الاصطناعي لتنظيم استخدام التقنية، وتطبيق التشريعات، ومتابعة الالتزام بها.
4. تطوير الإستراتيجيات الوطنية بما يتوافق مع المبادئ الدولية، مع مراعاة الظروف المحلية، لضمان الاستخدام المسؤول والمنظم للتقنية.
5. تطوير البنية التحتية الرقمية من شبكات إنترنت عالية السرعة، ومنصات بيانات حكومية مفتوحة، وبيئات رقمية آمنة ومحمية لدعم تطبيقات الذكاء الاصطناعي.
6. تحفيز الابتكار والبحث العلمي بتمويل المشاريع الوطنية، وتوفير منصة إلكترونية للترخيص الأكاديمي لاستخدام الذكاء الاصطناعي، مع تسهيل الإجراءات للباحثين والطلاب.

7. تعزيز التعاون الإقليمي والدولي مع المنظمات والجهات المصنعة لتسهيل الوصول إلى التقنيات والخبرات العالمية، والمشاركة في المبادرات الدولية لصياغة معايير موحدة وملزمة.
8. إشراك المجتمع المدني والقطاع الخاص في صياغة السياسات، وتطوير منظومة الذكاء الاصطناعي، وتعزيز الشراكات بين جميع الأطراف المعنية.
9. ضبط استخدام تقنيات الذكاء الاصطناعي في المؤسسات عبر الرقابة القانونية والتقنية، لضمان الشفافية، والمساءلة، والامتثال للأطر الأخلاقية.
10. تطوير منظومة تراخيص إلكترونية وميسرة لاستخدام الذكاء الاصطناعي، خاصة في القطاعات الأكاديمية والبحثية، لضمان سرعة الإجراءات وجودة الترخيص.

ورشة: التأمين على المخاطر السيبرانية

الجهة المنظمة

- شركة البركة للتأمين.

المتحدث الرئيسي

- علي الطير - رئيس قسم المبيعات.

عقدت شركة البركة للتأمين ورشة متخصصة بعنوان "تحويل التهديدات السيبرانية إلى أخطار يمكن إدارتها"، قدمها علي الطير - رئيس قسم المبيعات بالشركة، هدفت الورشة إلى رفع مستوى الوعي حول المخاطر السيبرانية المتزايدة التي تواجه البنية التحتية الحيوية في ليبيا، مع التركيز على قطاعات الاتصالات، والمصارف، والنفط، والغاز.

استعرضت الورشة المشهد الحالي للتهديدات السيبرانية العالمية والمحلية، وقدمت أمثلة واقعية لهجمات حدثت في ليبيا، مبرزةً الآثار المالية والتشغيلية المترتبة عليها، كما تم تسليط الضوء على الحلول التأمينية التي تقدمها شركة البركة كأداة إستراتيجية لإدارة هذه المخاطر، واختتمت الورشة بمجموعة من التوصيات العملية التي تهدف إلى تعزيز المرونة السيبرانية للمؤسسات الليبية.

المقدمة

افتتحت الورشة بكلمة ترحيبية ألقاها السيد علي الطير، الذي أكد خلالها على أهمية التأمين السيبراني في ظل التزايد السريع للهجمات الرقمية التي تستهدف بشكل مباشر البنية التحتية الحيوية للدولة. وأشار إلى التزام شركة البركة للتأمين بدعم جهود تعزيز الأمن السيبراني، من خلال تقديم حلول تأمينية متكاملة والمساهمة الفعالة في رفع مستوى الوعي والثقافة الأمنية عبر تنظيم ورش العمل والبرامج التدريبية المتخصصة. وقد شهدت الورشة حضور أكثر من 26 مشاركًا من مختلف القطاعات الحيوية في ليبيا، مما يعكس حرص الجميع على التعاون لمواجهة هذه التحديات المتزايد

محاور الورشة

بتقديم من علي الطير، غطت الورشة المحاور الرئيسية التالية:

المحور الأول: نبذة عن شركة البركة للتأمين

جرى استعراض خبرة الشركة في حلول التأمين المتخصصة، والتزامها بالتوعية بالمخاطر السيبرانية.

المحور الثاني: الغرض من الورشة والقطاعات المستهدفة

وُضّحت أهداف الورشة التي ركّزت على فهم مشهد التهديدات السيبرانية، وتحديد نقاط الضعف، والتعلم من الحوادث الحقيقية، وتطبيق إستراتيجيات فعالة لإدارة المخاطر.

المحور الثالث: مشهد التهديدات السيبرانية (2024 - 2025م)

قُدم تحليل للاتجاهات العالمية والإقليمية، مع التركيز على السياق الليبي والتحديات الخاصة به، مثل عدم الاستقرار السياسي والفجوات في التحول الرقمي.

المحور الرابع: نقاط الضعف والمخاطر في القطاعات الحيوية

- **قطاع الاتصالات:** سُلّط الضوء على المخاطر التي تواجه البنية التحتية للاتصالات، مع الإشارة إلى الهجوم على مركز بيانات الشركة الليبية للبريد والاتصالات وتقنية المعلومات القابضة (LPTIC) التابع لشركة ليبيا للاتصالات والتقنية واقعي.
- **القطاع المصرفي:** جرى استعراض المخاطر التي تواجه المؤسسات المالية، لا سيما منصات العملات الأجنبية، مع الإشارة إلى هجوم الحرمان من الخدمة (DDoS) الذي تعرض له مصرف ليبيا المركزي .
- **قطاع النفط والغاز:** جرى توضيح المخاطر الفريدة التي يواجهها هذا القطاع الإستراتيجي، بما في ذلك هجمات التصيد الاحتيالي، مع ذكر مثال هجوم التصيد الذي استهدف شركة زلاف للنفط والغاز.

المحور الخامس: حلول التأمين على المخاطر السيبرانية

فصّلت التغطيات الأساسية التي توفرها وثائق التأمين السيبراني، مثل تغطية تكاليف الاستجابة للحوادث، وانقطاع الأعمال، واستعادة البيانات، والمسؤولية تجاه الغير.

المحور الخامس: حلول مصممة خصيصًا للقطاعات

عُرضت كيفية تصميم وثائق تأمين لتلبية الاحتياجات الفريدة لقطاعات الاتصالات، والمصارف، والنفط، والغاز.

- **إستراتيجية التنفيذ وقصص النجاح:** شُرحت عملية تقييم المخاطر وتصميم التغطية، مع عرض دراسات حالة لنجاح تطبيق حلول التأمين السيبراني.
- **مشهد التهديدات المتطور:** بيّن علي الطير أن ليبيا، كغيرها من دول المنطقة، تواجه تصاعدًا مستمرًّا في حجم الهجمات السيبرانية وتعقيدها، وأشار إلى أن متوسط تكلفة اختراق البيانات في منطقة الشرق الأوسط وشمال أفريقيا بلغ 5.8 مليون دولار في عام 2024م، مع توقف الأعمال لمدد تصل في المتوسط إلى 23 يومًا، وأضاف أن العوامل المحلية، مثل حالة عدم الاستقرار السياسي وغيرها، تزيد من مخاطر تعرض البنية التحتية الحيوية لهجمات إستراتيجية تهدد الأمن الوطني.

أمثلة حقيقية وتأثيرها

كان عرض الأمثلة الحقيقية من أبرز نقاط القوة في الورشة، حيث تم تحليل:

- **هجوم مركز بياناتLTT LPTIC:** أظهر هذا الهجوم كيف يمكن أن تؤدي الهجمات المستمرة إلى تعطيل خدمات الاتصالات على مستوى الدولة، وأبرز أهمية الاستجابة المنسقة والدفاع المستمر.
- **هجوم DDoS على مصرف ليبيا المركزي:** أوضح هذا المثال كيف يمكن استهداف منصات مالية حيوية، وكيف أن تقنيات مثل الحجب الجغرافي (Geo-blocking) يمكن أن تكون استجابة أولية فعّالة، لكنها تسلط الضوء على الحاجة إلى حماية مختصة.

- **دور التأمين في إدارة المخاطر:** شدد على الطير على أن التأمين السيبراني لا يمنع الهجمات، ولكنه يوفر شبكة أمان مالية وتشغيلية حيوية، فالتغطية التأمينية لا تقتصر على التعويض المالي للخسائر، بل تشمل الوصول الفوري إلى فريق من الخبراء أيضًا؛ للمساعدة في الاستجابة للحوادث، وإدارة الأزمات، والتحقيقات الجنائية الرقمية، ما يقلل من زمن التعطل ويسرّع من عملية التعافي.

التوصيات

بناءً على محتوى الورشة والواقع الليبي، يمكن تلخيص التوصيات الرئيسية في النقاط التالية:

1. **تبني نهج استباقي:** على المؤسسات الليبية، لا سيما في القطاعات الحيوية، الانتقال من مجرد رد الفعل على الحوادث إلى بناء إستراتيجية استباقية لإدارة المخاطر السيبرانية، يكون التأمين جزءًا لا يتجزأ منها.
2. **الاستثمار في الوعي البشري:** نظرًا إلى أن العديد من الهجمات تبدأ من خطأ بشري، يجب تكثيف برامج التدريب والتوعية للموظفين على كافة المستويات؛ لمعرفة محاولات التصيد الاحتيالي والهندسة الاجتماعية والتصدي لها.
3. **تخصيص الميزانيات الكافية:** يجب أن توضح ميزانيات تقنية المعلومات الأهمية المتزايدة للأمن السيبراني. إن اعتبار التأمين السيبراني نفقات تشغيلية ضرورية، وليس ترفًا، هو تغيير جوهري في التفكير يجب أن تتبناه الإدارات العليا.
4. **تعزيز التعاون بين القطاعين العام والخاص:** لمواجهة التهديدات التي تستهدف البنية التحتية الوطنية، لا بد من وجود تعاون وثيق بين المؤسسات الحكومية والشركات الخاصة لتبادل المعلومات عن التهديدات وتنسيق جهود الاستجابة .
5. **إجراء تقييم شامل للمخاطر:** الخطوة الأولى لأي مؤسسة يجب أن تكون إجراء تقييم شامل للمخاطر بالتعاون مع خبراء، لتحديد نقاط الضعف وتصميم التغطية التأمينية المناسبة، التي تلائم حجم عملياتها وطبيعتها.


PresentationPurpose

ورشة: منصة الاستعلام NISSAباستخدام التقنيات الناشئة

الجهة المنظمة

- الهيئة الوطنية لأمن وسلامة المعلومات.

مقدم الورشة

- المهندس/ محمد شلابي.

عُقدت ورشة "منصة الاستعلام" NISSA يوم السبت الموافق 2 أغسطس 2025م، فجمعت نخبة من الخبراء والمتخصصين في مجال الأمن السيبراني والذكاء الاصطناعي، هدف اللقاء إلى استعراض الدور المحوري للذكاء الاصطناعي في تطوير إستراتيجيات الدفاع السيبراني، عن طريق النموذج التطبيقي منصة NISSA. قاد الورشة السيد محمد شلابي، فاستعرض للحضور المحاور الرئيسية التي ركزت على الانتقال من الأمن التفاعلي التقليدي إلى الأمن الاستباقي المدعوم بالذكاء الاصطناعي، مع تسليط الضوء على قدرة الذكاء الاصطناعي على تحليل كميات هائلة من البيانات بسرعة فائقة، والكشف المتقدم عن التهديدات غير المعروفة، وأتمتة الاستجابة للحوادث، ما يقلل بشدة من الأضرار المحتملة. وناقشت الورشة التحديات المصاحبة لهذه التقنيات، مثل المخاوف المتعلقة بالخصوصية والحاجة إلى الإشراف البشري. واختتمت الورشة بعرض مجموعة من الأدوات والمنصات المبتكرة، ومن ثم تقديم توصيات إستراتيجية للمؤسسات لتبني هذه التقنيات بفاعلية.

المقدمة

في وقت أصبحت فيه حياتنا مرتبطة بكل ما هو رقمي، لم يعد الأمن السيبراني مجرد تخصص تقني، بل صار ضرورة يومية لحماية كل ما نعدُّه مهمًّا: بياناتنا، وخصوصيتنا، ومؤسساتنا. ومع تزايد التهديدات الإلكترونية، لم يعد بالإمكان الاعتماد على الطرائق التقليدية وحدها، فهنا يأتي دور الذكاء الاصطناعي (Ai) بوصفه أداة ذكية تمنحنا خطوة استباقية في هذا السباق. من هذا المنطلق، كانت ورشة (منصة الاستعلام NISSA) مساحة لتبادل المعرفة والخبرات، واستكشاف كيف يمكن للتقنيات الناشئة أن تصنع مشهد الأمن السيبراني، ليس نظريًا فحسب، بل عن طريق أدوات عملية ودراسات حالة واقعية.

نبذة عن الجهة المنظمة

أدار جلسة الورشة السيد/ محمد شلابي، وهو شخصية متخصصة يتمتع بخبرة واسعة ومعرفة عميقة في مجالي الأمن السيبراني والذكاء الاصطناعي. يشغل المهندس محمد شلابي عضوية الفريق الوطني للاستجابة لطوارئ السيبرانية (LibyaCERT)، كما يتولى مسؤولية المساعد الذكي لدى الهيئة الوطنية لأمن وسلامة المعلومات، وهو حاصل على العديد من الشهادات المهنية المعتمدة في هذا المجال.

نُظمت هذه الورشة بالتعاون مع الهيئة الوطنية لأمن وسلامة المعلومات، وهي الجهة المسؤولة عن حماية البنية التحتية لتكنولوجيا المعلومات والاتصالات في ليبيا منذ تأسيسها عام 2013م. تعمل الهيئة على تعزيز منظومة الأمن السيبراني الوطني وحماية البيانات الحساسة، وقد أطلقت مؤخرًا "المساعد الذكي" وهو أداة متقدمة لدعم المتخصصين في هذا القطاع. وشهدت الورشة حضور عدد (11) شخصًا يمثلون جهات حكومية حيوية، وشركات من القطاع الخاص، إضافة إلى عدد من طلبة الجامعات، ويبين هذا الحضور المتنوع الاهتمام الوطني المتزايد بتطبيقات الذكاء الاصطناعي ودورها في تعزيز الأمن السيبراني.

محاور الورشة

صممت محاور الورشة لتغطي بصورة شاملة دور الذكاء الاصطناعي في الأمن السيبراني:

- المحور الأول: تحول المشهد السيبراني (من التفاعلية إلى الاستباقية).
- المحور الثاني: آليات عمل الذكاء الاصطناعي في ساحة المعركة السيبرانية.
- المحور الثالث: المزايا والتحديات (نظرة متوازنة).
- المحور الرابع: التقنيات الناشئة والأدوات المبتكرة.
- المحور الخامس: دراسات حالة وتطبيقات عملية.
- المحور السادس: استعراض منصة الاستعلام NISSA.
- المحور السابع: نظرة عامة على منصة الاستعلام NISSA.

تفصيل المحاور

المحور الأول: تحول المشهد السيبراني (من التفاعلية إلى الاستباقية)

حسب ما استعرضه مقدم الورشة فقد شهد العام الماضي زيادة بنسبة 38% في الهجمات السيبرانية، ما يؤكد أن الأساليب التقليدية لم تعد كافية. استعرض هذا المحور كيف يغير الذكاء الاصطناعي قواعد اللعبة، إذ يمكنه كشف التهديدات بسرعة تفوق الطرق التقليدية بـ 60 مرة. يتيح هذا التحول الإستراتيجي للمؤسسات القدرة على التعلم المستمر من الهجمات السابقة والتنبؤ بالتهديدات المستقبلية، مما يرسخ مفهوم الدفاع الاستباقي.

المحور الثاني: آليات عمل الذكاء الاصطناعي في ساحة المعركة السيبرانية

يرتكز دور الذكاء الاصطناعي على آليات محورية عدة:

- تقليل الإنذارات الكاذبة: بدلًا من إغراق المحللين بإنذارات غير حقيقية، يحدد الذكاء الاصطناعي المخاطر الفعلية بدقة عالية.
- الكشف المتقدم عن التهديدات: يتمكن الذكاء الاصطناعي من رصد الأنماط الخبيثة والتهديدات غير المعروفة في الزمن الحقيقي.
- تحليلات أمنية قائمة على البيانات: يحلل الذكاء الاصطناعي كميات ضخمة من سجلات الأمان لاكتشاف التهديدات الخفية التي قد تفوتها العين البشرية.
- الاستجابة التلقائية للحوادث: يمكن للأنظمة المدعومة بالذكاء الاصطناعي احتواء التهديدات والرد عليها على نحو فوري وتلقائي، مما يقلل من نافذة الهجوم.

المحور الثالث: المزايا والتحديات (نظرة متوازنة)

التطرق إلى كل من الجوانب الإيجابية والجوانب السلبية والتحديات:

الجوانب الإيجابية

- **كفاءة أعلى:** أتمتة المهام المتكررة توفر الوقت للمختصين للتركيز على التهديدات المعقدة.
- **دقة أعلى:** يساهم في تحسين معدلات اكتشاف التهديدات الحقيقية بنسبة تصل إلى 95%.

- **استجابة أسرع وتحليلات أعمق:** يتيح احتواء التهديدات في ثوانٍ ويوفر فهمًا أعمق لأنماط الهجمات.

الجوانب السلبية والتحديات

- **استخدام من قبل المهاجمين:** يمكن استغلال نفس التقنيات لتطوير هجمات أكثر تعقيدًا.
- **مخاوف الخصوصية:** يتطلب جمع كميات هائلة من البيانات الحساسة وتحليلها.
- **الحاجة إلى إشراف بشري:** لا تزال القرارات الحاسمة تتطلب حكمة العنصر البشري وخبرته.

المحور الرابع: التقنيات الناشئة والأدوات المبتكرة

استعرضت الورشة أحدث الأدوات المدعومة بالذكاء الاصطناعي، وتشمل:

- حماية الأجهزة الطرفي (Endpoint Protection): حلول متقدمة للكشف عن السلوكيات المشبوهة.
- أتمتة الاستجابة الأمنية (SOAR): أنظمة أكثر ذكاءً واستباقية للتعامل مع الحوادث.
- إدارة معلومات الأمان (SIEM): دمج الذكاء الاصطناعي لتحسين كشف التهديدات وتحليل السجلات.
- أدوات متخصصة: عرضت منصات مثل KaliGPT للمساعدة في اختبار الاختراق، Blue Teamg Defender GPT لتعزيز قدرات فرق الدفاع .

المحور الخامس: دراسات حالة وتطبيقات عملية

عرضت تجارب واقعية لمؤسسات عالمية مثل IBM Watson Corden Pharma، وأظهرت هذه الحالات كيف ساهم الذكاء الاصطناعي في حماية بيانات حساسة، وتقليل الهجمات الناجحة بنسبة 70%، وتوفير ملايين الدولارات سنويًا.

المحور السادس: استعراض منصة الاستعلامNISSA

كان من المخطط أن يتضمن هذا المحور السادس جلسة تطبيقية مباشرة، تتيح للمشاركين تجربة منصة NISSAعمليًا والتفاعل مع خصائصها في بيئة محاكاة واقعية، لكن ضيق الوقت الناتج عن تأخر انطلاق الورشة وتزامنها مع جدول ورشة أخرى حال دون تنفيذ هذا الجزء كما كان مرسومًا. بدلًا من ذلك، تواصلنا مع مقدم الورشة م. محمد شلابي، وطلبنا منه الرابط المباشر لمنصة الاستعلام (NISSA) لتجربة حقيقية لهذه المنصة، وكذلك تكملة الاستفسار عن آلية عملها.

المحور السابع: نظرة عامة على منصة الاستعلام NISSA

الهدف الرئيسي للمنصة

يكمن الهدف الرئيسي لـ Nissa AI في تقديم الدعم المعرفي والتفاعلي حول جميع الجوانب المتعلقة بأمن المعلومات في ليبيا. بمعنى آخر، هي أداة تهدف إلى نشر الوعي، وتوفير المعلومات الدقيقة والموثوقة عن سياسات الهيئة الوطنية لأمن وسلامة المعلومات، وإجراءاتها، وخدماتها، ومبادراتها.

أبرز خصائصها التقنية

تشمل أبرز خصائصها التقنية ما يلي:

- معالجة اللغة الطبيعية (NLP): القدرة على فهم اللغة العربية والإنجليزية المستخدمة في استفساراتك وتحليلها.
- استرجاع المعلومات: إمكانية الوصول إلى المعلومات المخزنة من مصادر الهيئة الوطنية لأمن وسلامة المعلومات.
- توليد النصوص: توليد ردود دقيقة وواضحة باللغة العربية والإنجليزية.
- التعلّم المستمر: تحدّث قاعدة المعرفة باستمرار بناءً على المعلومات الجديدة الصادرة من الهيئة.

الجهات المستهدفة باستخدامها

تهدف Nissa AI إلى خدمة مجموعة واسعة من الجهات، وتشمل:

- **المواطنون:** لتزويدهم بالمعلومات حول كيفية حماية أنفسهم من التهديدات الأمنية الرقمية.

- **المؤسسات الحكومية:** لتوفير الدعم والمعلومات اللازمة لتطبيق السياسات والمعايير الوطنية لأمن المعلومات.
- **القطاع الخاص:** لتوفير الإرشادات حول كيفية تأمين أنظمتهم وبياناتهم.
- **الباحثون والطلاب:** لتوفير مصدر موثوق للمعلومات حول أمن المعلومات الوطني.
- **المهنيون في مجال أمن المعلومات:** لتقديم معلومات متخصصة حول السياسات والإجراءات الأمنية.

التوصيات

في ضوء ما طُرح في الورشة من عرض تقديمي وملاحظات الحاضرين، برزت مجموعة من التحديات التي تواجهها ليبيا في تبنّي تقنيات الذكاء الاصطناعي لدعم الأمن السيبراني، ومن أبرز هذه التحديات: محدودية البنية التحتية التقنية، وضعف التمويل المستدام للبحث والتطوير، وغياب الأطر التشريعية المواكبة، ونقص الكفاءات المتخصصة، وبناءً على ذلك نوصي بما يلي:

1. **تعزيز الاستثمار في البحث والتطوير:** ينبغي توجيه دعم مستمر لمبادرات البحث في مجالات الذكاء الاصطناعي والأمن السيبراني، بما يواكب التطورات العالمية ويوفر حلولًا محلية تلائم السياق الليبي.

2. **تأهيل الكوادر البشرية وبناء القدرات الوطنية**: من الضروري الاستثمار في تدريب المتخصصين، وطلبة الجامعات، والعاملين في المؤسسات الحكومية والخاصة، على مفاهيم وتطبيقات الذكاء الاصطناعي في المجال السيبراني؛ لتقليص الفجوة المعرفية، وضمان الاستخدام الفعّال للتقنيات.

3. **تطوير السياسات والتشريعات**: يتطلب الأمر إعداد أطر تنظيمية وتشريعية واضحة تنظم استخدام الذكاء الاصطناعي، بما يضمن تحقيق التوازن بين تطويع هذه التقنيات لخدمة الأمن الوطني، وحماية الخصوصية والحقوق الرقمية للمواطنين.

4. **تعزيز التعاون المحلي والدولي**: تشجيع الشراكات بين المؤسسات الوطنية، وتوسيع قنوات التعاون مع المراكز البحثية الدولية والجهات المتخصصة في الذكاء الاصطناعي والأمن السيبراني، بهدف تبادل الخبرات والمعلومات ومواكبة أفضل الممارسات.

5. **التركيز على الحلول الاستباقية بدلًا من التفاعلية**: ينبغي تبنّي منهجيات وتقنيات تُمكن من الكشف المبكر عن التهديدات وتوقّع الهجمات، بدلًا من الاقتصار على التعامل مع الحوادث بعد وقوعها، مما يعزز مناعة الفضاء السيبراني الوطني.

ورشة: مشاركة أصحاب المصلحة في نقاشات مستقبل النطاق الوطني

المقدمة

أُقيمت على هامش منتدى حوكمة المعلوماتية جلسة نقاش بعنوان "**مشاركة أصحاب المصلحة في نقاشات مستقبل النطاق الوطني .LY**"، التي مثّلت فرصة حقيقية للتشاور والانفتاح على الآراء المختلفة ومقترحات الأطراف المعنية بإدارة النطاق الوطني العلوي لليبيا (ccTLD). وقد هدفت الجلسة إلى مراجعة السياسات الحالية الخاصة بإدارة النطاق، ومناقشة

التحديات والفرص، وبحث آليات تطوير الحوكمة بما يضمن الاستخدام الأمثل للنطاق في خدمة التنمية الرقمية والاقتصادية في ليبيا.

شهدت الجلسة مشاركة ممثلين عن الهيئة العامة للاتصالات والمعلوماتية، شركة ليبيا للاتصالات والتقنية (LTT)، شركة العنكبوت الليبي، المؤسسة الليبية للتقنية، مجتمع الإنترنت - ليبيا، ومجموعة من الخبراء وأصحاب العلاقة من القطاعين العام والخاص والمجتمع المدني. وقد دار النقاش حول المحاور التالية:

- أهمية النطاق الوطنيLY. بوصفه أصلًا رقميًّا وسياديًّا يمكن أن يكون مصدر دخل وواجهة رقمية للدولة الليبية، مع استعراض تاريخه وتطوره منذ 2005م.
- دور الهيئة في تولي مسؤولية إدارة النطاق بدلًا من الشركة العامة للبريد، وضرورة مراجعة سياسة إدارة النطاق وتحديثها بما يناسب أفضل الممارسات العالمية.
- التحديات الحالية المتمثلة في ضعف الوعي المجتمعي، وغياب جهة واضحة للدعم الفني والتقني، والتداخل بين الجهات الرسمية حول إدارة الامتدادات مثل.gov.ly .

مقترحات المشاركين شملت:

- عقد لقاء سنوي رسمي يجمع أصحاب المصلحة للنقاش وتبادل التجارب.
- تطوير السياسة الحالية بإشراك جميع أصحاب المصلحة وفق نموذج bottom-up.
- إلزام المؤسسات الوطنية باستخدام النطاق الوطني في مواقعها الإلكترونية.
- تعزيز التوعية المجتمعية بأهمية استخدام .LY.
- تكوين لجنة استشارية دائمة تضم ممثلين عن الجهات الحكومية والشركات والمجتمع المدني.

اختُتمت الجلسة بالتأكيد على أهمية المضي قدمًا في بناء نموذج حوكمة تشاركي ومستدام، يعزز من سيادة الدولة الرقمية، ويدعم مسار التحول الرقمي في ليبيا.

المشاركون البارزون

- القطاع الحكومي: الهيئة العامة للاتصالات والمعلوماتية.
- القطاع الخاص: شركة ليبيا للاتصالات والتقنية (LTT)، شركة العنكبوت الليبي.

- المجتمع المدني: المؤسسة الليبية للتقنية، مجتمع الإنترنت - ليبيا.

محاور الورشة

المحور الأول: أهمية المنتدى

أثنى الحضور على أهمية هذا المنتدى، فهو منصة حقيقية تجمع أصحاب المصلحة المعنيين بإدارة النطاق الوطني الليبي (ly.)، إذ يُعد المنتدى أول لقاء من نوعه يشمل كافة الأطراف المعنية بحوكمة (ccTLD) الخاص بليبيا.

لقد مثّل المنتدى فرصة جوهرية لفتح باب التشاور والنقاش المباشر بين ممثلي الجهات الحكومية، ومقدمي الخدمة، والخبراء، والمجتمع المدني، بشأن السياسات الحالية المتعلقة بإدارة النطاق، وتحديد أوجه القصور والتحديات، واقتراح آليات تطوير تواكب التغيرات التقنية والاحتياجات الوطنية. ويأتي هذا التوجه انسجامًا مع سياسات الهيئة التي تؤكد على أهمية التشاور مع أصحاب المصلحة، إذ هو عنصر أساسي في صياغة السياسات العامة ذات الصلة بالبنية التحتية الرقمية والسيادة التقنية وتحديثها.

المحور الثاني: تاريخ LY. وأهميته

كان تسجيل أول اسم نطاق تحت النطاق الوطني العلوي لليبيا (ly.) في 25 فبراير 2005م، وهو تاريخ يُعد محطة مفصلية في مسار السيادة الرقمية الليبية. قبل هذا التاريخ، كانت ليبيا تواجه عقوبات دولية حالت دون إدارتها المباشرة لنطاقها الوطني.

وفي إطار سعي الدولة الليبية لاستعادة إدارتها الرقمية، نُقلت إدارة النطاق إلى شركة ليبيا للاتصالات والتقنية (LTT)، التي تولت مسؤولية تشغيله وتوفير الخدمات المتعلقة به داخليًّا وخارجيًّا، بالتعاقد مع جهات وسيطة لتسهيل وصول المستخدمين الدوليين. ومن المعروف أن لكل دولة نطاقًا علويًّا خاصًّا بها (ccTLD)؛ يُستخدم لتمييز وجودها الرقمي، ورمز ليبيا في هذا النظام هو (ly.)، الذي لا يمثل مجرد عنوان إلكتروني، بل أصل رقمي سيادي له أبعاد قانونية واقتصادية وإستراتيجية.

أشار الحضور إلى أن النطاق الوطني الليبي يمتلك إمكانات اقتصادية كبيرة، ويمكن أن يكون مصدر دخل مهم للدولة في حال استغلاله على نحو منظم وفعّال، لا سيما مع ارتفاع الطلب على امتدادات النطاقات المميزة حول العالم، وارتباط بعض العلامات التجارية العالمية بـ(ly.)، مثل "bit.ly"، ما يعزز من قيمة هذا الأصل الرقمي في السوق الدولية.

المحور الثالث: الوضع الحالي وإدارة نطاق (ly.)

الهيئة العامة للاتصالات والمعلوماتية هي الجهة المسؤولة رسميًّا عن تنظيم النطاق الوطني العلوي (ccTLD) لليبيا وإدارته، ويأتي هذا التحول في إطار سعي الدولة إلى تعزيز الحوكمة الرقمية، وترسيخ مفهوم السيادة على الفضاء الإلكتروني الليبي.

مع وجود سياسة منشورة حاليًّا لإدارة النطاق، فإن المشاركين في الجلسة أكدوا على أن هذه السياسة بحاجة إلى مراجعة وتحديث، بما يوضح التغيرات التقنية والتحديات التشغيلية، ويستفيد من تجارب الدول الأخرى وأصحاب الخبرة في المجال. ويُنظر إلى عملية تطوير السياسة على أنها أولوية لضمان إدارة فعّالة ومستدامة لهذا الأصل الرقمي الحيوي.

وفي السياق ذاته، ما زال لشركة ليبيا للاتصالات والتقنية (LTT) دور تنفيذي وتقني ضمن المنظومة، فقد عملت على تطبيق أفضل الممارسات المعمول بها دوليًّا، وسعت إلى تسهيل عمليات التسجيل والوصول إلى النطاقات من خارج ليبيا؛ بالتعاقد مع شركة العنكبوت الليبي، التي تعمل وسيطًا تقنيًّا وتجاريًّا بين المستخدمين الدوليين والنظام الوطني.

وشدد الحضور على أن إدارة النطاق الوطني لا يمكن أن تكون فاعلة دون وجود منظومة حوكمة متكاملة، تشمل الجهات الحكومية (الجهة المنظمة)، والشركات المنفذة، إلى جانب تمثيل حقيقي للمجتمع المدني، والقطاع الخاص، والمستخدمين النهائيين. وقد جرى التأكيد على أن السياسات المستقبلية يجب أن تُبنى وفق نموذج تشاركي (bottom-up)، يضمن إشراك جميع أصحاب المصلحة في صياغة القرارات وتحديد الأولويات.

التوصيات

1. **لقاء سنوي رسمي:** اقترح المشاركون عقد لقاء سنوي يجمع أصحاب المصلحة كافة لمناقشة التحديات ومشاركة التجارب، على أن يكون هذا المنتدى التأسيسي هو الخطوة الأولى.
2. **سياسة bottom-up:** الدعوة إلى تطوير السياسة الحالية، بإشراك الجهات المعنية من أسفل إلى أعلى، وتضمين المجتمع المدني والمستخدمين والقطاع الخاص في صناعة القرار.
3. **التوعية والتدريب:** تعزيز الجهود التوعوية بأهمية النطاق الوطني، لا سيما للجهات الحكومية والقضائية والأكاديمية، وتقديم تدريبات مستمرة للموظفين الجدد.
4. **التوصية باستخدام LY.:** طرح مقترح بتوصية المؤسسات الوطنية، سواء كانت حكومية أو تعليمية أو تجارية، باستخدام النطاق الوطني في مواقعها الرسمية، كما هو معمول به في بعض الدول.
5. **التنظيم والرقابة:** الدعوة إلى تقنين تسجيل النطاقات ليكون مقتصرًا على الليبيين أو المقيمين داخل ليبيا، ومنع المتاجرة العشوائية بالنطاقات.
6. **إنشاء لجنة استشارية:** اقترح أحد المشاركين إنشاء لجنة تمثل كافة أصحاب المصلحة، تعمل كجسم مرجعي يقدم التوصيات، ويساهم في تنظيم اللقاءات السنوية ومتابعة تنفيذ السياسات.
7. تُعد هذه الجلسة خطوة أولى نحو بناء نموذج وطني متكامل لحوكمة الإنترنت، يستند إلى الشراكة، ويعزز من حضور ليبيا الرقمي عالميًا.
8. التأكيد على أهمية الحوكمة والتنسيق بين جميع الأطراف.
9. التأكيد على أن النطاق ليس خدمة تقنية فقط، بل هو عنصر سيادي واقتصادي مهم.
10. دعوة إلى الاستمرار في الحوار واللقاءات الدورية لضمان تطوير قطاع الإنترنت في ليبيا.

ورشة: الرقابة على تقنية المعلومات

المقدمة

في إطار تطوير قدرات الجهات الرقابية وتعزيز فاعلية الدور الرقابي في مجال الحوكمة الرقمية، نُظمت جلسة فنية بعنوان "الرقابة على تقنية المعلومات"، قدمها الأستاذ/ عبد الحميد الديب من مكتب تقنية المعلومات بديوان المحاسبة. هدفت هذه الجلسة إلى تسليط الضوء على المفاهيم الأساسية لرقابة تقنية المعلومات، وبيان أهميتها في ضمان الكفاءة التشغيلية وحماية البنية التحتية الرقمية، واستعراض المنهجيات المتبعة في تنفيذ هذا النوع من الرقابة، إلى جانب عرض أبرز المعايير الدولية والمحلية التي تستند إليها العملية الرقابية، والضوابط الفنية والتنظيمية المعتمدة.

استُهلت الجلسة بعرض تاريخي حول نشأة الرقابة على تقنية المعلومات في ليبيا، فأوضح المحاضر أن هذا التخصص بدأ يأخذ شكله المؤسساتي في سنة 2012م، عن طريق مبادرة أطلقتها مؤسسة IDI، وهي مؤسسة دولية تُعنى بتطوير قدرات الأجهزة الرقابية في القارات إفريقيا وآسيا وأوروبا. وقد ساهمت هذه المبادرة في بناء فهم أعمق لمفهوم الرقابة التقنية، وتبادل التجارب والخبرات بين الدول. أكد الأستاذ عبد الحميد أن الرقابة على تقنية المعلومات ليست مجرد تقييم لوجود أجهزة أو أنظمة تشغيل، بل هي عملية شاملة تتضمن فحصًا دقيقًا للبنية التحتية الرقمية للجهة، وتحليلًا للأدلة والبيانات المرتبطة بالأداء التقني، بهدف التأكد من فاعلية الأنظمة، وضمان أمن المعلومات، وتعزيز الامتثال للمعايير المعتمدة. ثم إنه شدد على أن هذه الرقابة تُعد أداة محورية في تعزيز الشفافية، والحد من المخاطر، وضمان استمرارية تقديم الخدمات العامة بكفاءة.

محاور الورشة

المحور الأول: مفهوم الرقابة على تقنية المعلومات وأهدافها

جرى في هذه الجلسة توضيح أن الرقابة على تقنية المعلومات تهدف إلى ضمان توافر المعلومات عند الحاجة إليها، والحفاظ على سريتها من الوصول غير المصرح به، وضمان نزاهتها

حتى لا يجري التلاعب بها أو تغييرها دون تفويض. وتُعرف هذه المبادئ الثلاثة في علم أمن المعلومات بـ: التوفر (Availability)، السرية (Confidentiality)، والنزاهة (Integrity). وأشار المحاضر إلى أن الجهات العامة تعتمد على منظومات تقنية مختلفة لتنفيذ أعمالها اليومية، ما يجعل من الضروري فحص هذه المنظومات وضمان مطابقتها للمعايير الأمنية، إضافة إلى تحليل مدى اعتماد الجهة على تلك الأنظمة، وما إذا كانت تتّبع ممارسات فعّالة لحمايتها وصيانتها.

المحور الثاني: فئات الأصول الخاضعة للرقابة

تناولت الجلسة فئات الأصول التي قُيّمت في عملية الرقابة، والتي صُنّفت إلى أربع فئات رئيسية، وهي:

- **أصول المعلومات:** وتشمل جميع أشكال البيانات والمحتوى الرقمي الذي تنتجه الجهة أو تعتمد عليه.
- **الأصول التقنية:** مثل أجهزة الحاسوب والخوادم والشبكات وأنظمة التشغيل، التي تمثل البنية التحتية لتقنية المعلومات.
- **العنصر البشري:** ويشمل العاملين داخل الجهة ومدى وعيهم والتزامهم بسياسات الأمن السيبراني.
- **أصول الخدمة:** أي المكونات التي تُمكن من تقديم الخدمات الرقمية للمستفيدين أو الجهات الأخرى.
- وقد أوضح المحاضر أن الرقابة لا تكتفي بفحص النظام فحسب، بل تشمل السياق المؤسسي كله، بما في ذلك ثقافة الأمن السيبراني، والإجراءات التشغيلية، ومدى وجود خطط استجابة للطوارئ.

المحور الثالث: المنهجية المتبعة في تنفيذ الرقابة

عرض المحاضر الخطوات العملية المتبعة عند تنفيذ عملية رقابة تقنية المعلومات داخل الجهات العامة، التي تبدأ بمرحلة التقييم المبدئي للجهة لفهم طبيعة عملها، والأدوار التقنية التي تعتمد عليها، وتحديد الأولويات العامة.

تلي ذلك مرحلة تقييم المخاطر، التي يجري فيها حصر نظم المعلومات المستخدمة داخل الجهة، وتحديد الأنظمة الحساسة التي تُعد ذات أهمية عالية لاستمرارية العمل، ثم تُحلّل المخاطر المحتملة التي قد تؤثر على هذه الأنظمة، وترتب أولويات المراجعة بناءً على درجة الخطورة والتأثير المحتمل. بعدها، تنتقل العملية إلى مرحلة جمع الأدلة، باستخدام أدوات متعددة مثل إجراء مقابلات مع العاملين في الجهة، وتوزيع استبيانات، ومراجعة الإجراءات المكتوبة، إضافة إلى تحليل سير العمليات باستخدام المخططات الانسيابية (flowcharts).

بعد ذلك تأتي مرحلة اختبار الضوابط التقنية، التي تشمل اختبار أنظمة الحماية التقنية ومدى فاعليتها، والتحقق من أن الضوابط المعتمدة تشمل ضوابط وقائية (لمنع الخلل)، وضوابط كشفية (للكشف عن المشكلات في حال حدوثها)، وضوابط تصحيحية (للتعامل مع الخلل بعد وقوعه). كما يجري التحقق من مدى امتثال التطبيقات والأنظمة لمتطلبات الأمن السيبراني. تُختتم المنهجية بإعداد تقرير نهائي شامل، يتضمن النتائج التي جرى التوصل إليها، والتوصيات المتعلقة بمعالجة الثغرات والتحسينات المقترحة، ثم يقدم إلى الإدارة العليا في الجهة المعنية.

المحور الرابع: المعايير المعتمدة في الرقابة

أكد المحاضر أن ديوان المحاسبة يستند في عملية الرقابة إلى معايير دولية معتمدة، أبرزها: معيار ISO/IEC 27001، الذي يُعد إطارًا متكاملًا لإدارة أمن المعلومات داخل المؤسسات. معايير إدارة الخدمات التقنية وأمن نظم المعلومات. أطر العمل الصادرة عن مؤسسة ISACA، ومنها إطار إدارة مخاطر تكنولوجيا المعلومات، وإطار الممارسات المهنية لتقنية المعلومات. وفي السياق المحلي، أشار إلى الجهود المستمرة لتطوير معايير وطنية للرقابة على تقنية المعلومات، التي تأخذ في الاعتبار خصوصية السياق الليبي، والاحتياجات الفعلية للجهات العامة، والتحديات التي تواجهها.

المحور الخامس: أنواع الضوابط الرقابية

تطرقت الجلسة إلى تصنيف الضوابط الرقابية إلى نوعين رئيسيين:

- **ضوابط عامة:** وهي الضوابط التي تنطبق على البنية التحتية والممارسات العامة في الجهة.
- **ضوابط خاصة بالتطبيقات:** وتُقسم إلى ثلاث مراحل:
  - ضوابط المدخلات، للتأكد من دقة البيانات التي تدخل النظام وسلامتها.

- ضوابط العمليات، لضمان أن النظام ينفذ العمليات كما هو مخطط لها.
- ضوابط المخرجات، للتحقق من عد التلاعب بالنتائج وأنها تُرسل إلى الجهات المستفيدة فقط.

الخاتمة والتوصيات

في ختام الجلسة، أكد الأستاذ/ عبد الحميد الديب أن الرقابة على تقنية المعلومات صارت اليوم عنصرًا أساسيًّا لا يمكن تجاهله في إطار الحوكمة الرشيدة وحماية المال العام. وأوضح أن فاعلية هذه الرقابة تعتمد اعتمادًا كبيرًا على بناء كوادر رقابية مؤهلة، واتباع منهجيات دقيقة تستند إلى المعايير الدولية، مع مراعاة الخصوصية المؤسسية والسياق المحلي. وقد خلصت الجلسة إلى عدد من التوصيات المهمة، من أبرزها:

1. ضرورة الاستمرار في بناء قدرات العاملين وتطويرها في مجال رقابة تقنية المعلومات، بالتدريب والتأهيل المستمرين.
2. التأكيد على تطبيق المعايير الدولية والمحلية بطريقة متوازنة؛ لضمان شمولية الرقابة وفاعليتها.
3. إعطاء أهمية كبيرة لعملية تحليل المخاطر عند التخطيط للمراجعات الرقابية، لتوجيه الجهد نحو الأنظمة الأكثر حساسية.
4. التركيز على مبادئ أمن المعلومات (التوافر - السرية - النزاهة) فهي أعمدة أساسية في عمليات التقييم.

ورشة: عرض شامل للسياسات والإستراتيجيات الصادرة عن الهيئة العامة للمعلومات

المقدمة

افتتحت الورشة بكلمة ترحيبية من م. منير، الذي قدّم لمحة عن الهيئة العامة للمعلومات، متناولًا تاريخ تأسيسها وهيكلها التنظيمي، واستعرض الرؤية والرسالة والقيم التي ترتكز عليها الهيئة كما أوضح دورها ضمن المنظومة الوطنية للمعلوماتية بالتعاون مع مؤسسات الدولة ذات العلاقة. وقد تضمنت المقدمة عرضًا توضيحيًّا للفروقات بين مفاهيم حوكمة المعلومات، وحوكمة البيانات، والنفاذية الرقمية، مع التنويه بأهمية هذه المفاهيم في تطوير منظومة الخدمات الحكومية.

الهيئة جزء من المؤسسات المعلوماتية إلى جانب:

- الهيئة العامة للاتصالات والمعلوماتية.

- الهيئة الوطنية لأمن وسلامة المعلومات.
- إضافة إلى المؤسسات الأخرى الداعمة في هذا المجال.

أهداف الورشة

- عرض السياسات والوثائق الصادرة عن الهيئة مؤخرًا.
- تسليط الضوء على التوجهات الوطنية للتحول الرقمي.
- دعوة مراكز المعلومات للمساهمة في تنفيذ السياسات.

محاور الورشة

المحور الأول: السياسات الوطنية للتحول الرقمي والتنمية الرقمية

الإستراتيجية الوطنية للتحول الرقم (2023 - 2030م)

أصدرتها الهيئة في هذا الجانب بالتعاون مع المجلس الوطني للتطوير الاقتصادي والاجتماعي، فاعتمدت رئاسة الوزراء هذه الإستراتيجية في المدة السابقة، أمّا حاليًّا فتعمل الهيئة على وضع مصفوفة إجراءات لتنفيذ هذه الإستراتيجية بالتعاون مع مجموعة من المؤسسات الحكومية، وتحديدًا أصحاب المصلحة، وتهدف إلى تحقيق تحول رقمي شامل يشمل:

- حكومة رقمية فعّالة.
- اقتصادًا رقميًّا تنافسيًّا.
- مجتمعًا رقميًّا شاملًا.
- جدول الأعمال الوطنية للتنمية الرقمية.
- وثيقة تنفيذية للإستراتيجية تحتوي على إجراءات ومؤشرات قياس الأداء.

المحور الثاني: الأطر التنظيمية والتقنية في تعزيز الخدمات الرقمية

الوثائق الصادرة

- الإطار التنظيمي لإنترنت الأشياء.
- الإطار المقترح لجودة الخدمات الرقمية.

- الدليل الاسترشادي للمواقع والمنصات الحكومية.

تهدف هذه الوثائق إلى تحسين جودة الخدمات الرقمية وتوحيد المعايير.

المحور الثالث: حوكمة البيانات والنفاذية الرقمية

الوثائق الصادرة

- السياسة الوطنية لحوكمة البيانات الحكومية.
- الدليل الوطني للبيانات الحكومية، الذي يعدّ من أوائل الوثائق الصادرة في حوكمة البيانات.
- السياسة الوطنية للنفاذية الرقمية (خاصة بذوي الإعاقة وكبار السن).

نفّذت في المؤسسات الحكومية دورات تدريبية عدة لشرح هذه الوثائق، وجميعها موجودة على الموقع الإلكتروني للهيئة العامة للمعلومات: https://www.gia.gov.ly.

المحور الرابع: المبادرات والقوانين

مشروع الهوية الرقمية

تسعى الهيئة في اعتماده إلى أن يتضمن الهوية الرقم الوطني، ورقم جواز السفر، ورقم الهاتف. وكلما زادت البيانات الشخصية كانت الهوية الرقمية قوية.

وفي هذا السياق، في وقت سابق انطلق مشروع خاص بالمرتبات، بالتعاون مع مصرف ليبيا المركزي ووزارة المالية والهيئة العامة للمعلومات، وقد اعتمد هذا المشروع على الهوية الرقمية.

المنصات الحكومية

تسعى الهيئة إلى إصدار مجموعة من المنصات الحكومية، من ضمنها:

- منصة البيانات المفتوحة التي سيجري إطلاقها قريبًا.
- مشاركة المواطنين في صنع القرار عن طريق المنصات الرقمية في مجال التحول الرقمي.
- تحسين جودة الخدمات الرقمية وضمان الوصول. يوجد إطار تنظيمي في هذا الموضوع صدر في وقت سابق.

في سنة 2030م سيصل الإنترنت إلى 90% من السكان، وستكون سرعته عالية، و80% من الخدمات الإلكترونية يجب أن تكون مرقمنة، إذ إن نسبة رضا المواطنين على الخدمات الإلكترونية تبلغ 75%، وسيُدرّب 200 ألف موظف حكومي على المهارات الرقمية.

قوانين قيد الإعداد أو التعديل والإصدار

- قانون الاتصالات.
- قانون المعاملات الإلكترونية (مسودة).
- قانون المعلومات المتعلقة بالنشر الإلكتروني.
- قانون الأرشفة وإدارة الوثائق الحكومية (سياسة).
- قانون مشتريات الحكومية الإلكترونية (توجد لائحة بذلك مرتبطة بمنصة المشتريات الحكومية الإلكترونية).
- قانون الجرائم الإلكترونية وحماية أمن المعلومات (صدر قانون رقم 5 عن البرلمان الليبي في المدة السابقة).
- قانون حماية البيانات الشخصية.
- قانون النفاذ للمعلومات.

الهيئة لم تتوقف على العمل على إصدار سياسات وفق اختصاصها وصلاحياتها، وهذه السياسات ستتحول إلى قوانين عند استقرار وضع الدولة.

المحور الخامس: التحديات والأسئلة المطروحة

مداخلة من موظف بوزارة التعليم: نجد صعوبة في فرض حماية على البرامج الخارجية.

- الرد: الهيئة الوطنية لسلامة وأمن المعلومات تصدر شهادات امتثال لحماية البيانات وتتحقق من النظام وسلامته.

مداخلة من موظف بمركز المعلومات والتوثيق السياحي - م. عبد الرؤوف امبيس: عدم القدرة على الحصول على نطاق gov.ly.

- الرد: جرت مخاطبة الجهات المختصة ولم نتلق أي استجابة، ما أدى إلى عدم مقدرتنا على مشاركة الأعمال مع الشركات وتوقف بعض المشاريع.

- الرد: الحصول على نطاق gov.ly به صعوبة نظرًا لأهميته وحساسيته؛ لأنه يمثل الجهة الحكومية، والمسؤول على منح هذا الامتداد هو رئاسة الوزراء.

مداخلة من موظف بوزارة التعليم، مديرة مركز المعلومات والتوثيق أ. هويدا الشيباني: رفض بعض الجهات التابعة للتعليم مشاركة البيانات؟

- الرد: مكتب مراقبة الأنظمة المعلوماتية في هيئة الرقابة الإدارية هو المسؤول عن مراقبة عملية الامتثال في تبادل البيانات ومشاركتها، بالتنسيق مع اللجنة العليا للنظام الوطني للمعلومات.

المحور السادس: الإصدارات والقوانين

اعتمدت ثلاث وثائق رئيسية صادرة عن الهيئة من قبل مجلس رئاسة الوزراء ووُقّعت، وهي:

- الإستراتيجية الوطنية للتحول الرقمي.
- الأجندة الوطنية للتنمية الرقمية.
- السياسة الوطنية للنفاذية الرقمية.

إصدارات ضمن محور التحول الرقمي والتنمية الرقمية

اسم الوثيقة/السياسة	الهدف	الملاحظات
الإستراتيجية الوطنية للتحول الرقمي(2023-2030)	خارطة طريق وطنية شاملة للتحول الرقمي	اعتمدت من رئاسة مجلس الوزراء
الأجندة الوطنية للتنمية الرقمية	وثيقة تنفيذية للإستراتيجية تشمل الإجراءات ومؤشرات الأداء	تُكمل الإستراتيجية
الإطار التنظيمي لإنترنت الأشياء	تنظيم استخدام تقنيات داخل القطاع العام	منشور ومتاح
الإطار المقترح لجودة الخدمات الرقمية	تحسين جودة الخدمات الرقمية الحكومية	منشور

الدليل الاسترشادي للمواقع والمنصات الحكومية	توحيد معايير تصميم المواقع الحكومية	متاح للتنفيذ

سياسات وأدلة إضافية قيد الإعداد أو الاعتماد

اسم الوثيقة/السياسة	الهدف	الملاحظات
السياسة الوطنية للبيانات المفتوحة	تمكين نشر البيانات الحكومية للعموم	ستصدر قريبًا
إستراتيجية الهيئة لإدارة الأزمات والكوارث	تنظيم استجابة الهيئة للطوارئ	قيد الاعتماد

مشروعات قوانين متعلقة بالمجال المعلوماتي بشراكة مع جهات أخرى

اسم القانون	الجهة الشريكة/ الداعمة	الملاحظات
قانون حماية البيانات الشخصية	مجلس الحريات وحقوق الإنسان	جاهز ما عدا فصل العقوبات
قانون المعاملات الإلكترونية	البرلمان	المسودة موجودة
قانون الاتصالات	هيئة الاتصالات	موجود
قانون النفاذ للمعلومات	الهيئة العامة للمعلومات	قيد المتابعة
قانون الأرشفة والوثائق	الهيئة العامة للمعلومات	توجد سياسة ويجري تطوير القانون
قانون المشتريات الحكومية الإلكترونية	وزارة الاقتصاد - منصة المشتريات	توجد لائحة حالية
قانون الجرائم الإلكترونية	البرلمان	صدر باسم قانون رقم 5

إصدارات ضمن محور حوكمة البيانات والنفاذية الرقمية

اسم الوثيقة/السياسة	الهدف	الملاحظات
السياسة الوطنية لحوكمة البيانات الحكومية	تنظيم إدارة البيانات داخل المؤسسات الحكومية	ضمن السياسات الأساسية للتنفيذ
الدليل الوطني للبيانات الحكومية	مرجع فني لتوصيف البيانات وتصنيفها	من أوائل الوثائق الصادرة
السياسة الوطنية للنفاذية الرقمية	تسهيل الوصول الرقمي لذوي الإعاقة وكبار السن	تستند إلى معايير دولية

المحور السابع: التوصيات

1. تفعيل إستراتيجية التحول الرقمي والسياسات الوطنية ضمن كل القطاعات.
2. تعزيز التدريب والتوعية بسياسات الحوكمة.
3. دعم تنفيذ الإستراتيجية الرقمية من كل الشركاء.
4. اعتماد السياسات قيد المراجعة والإصدار الرسمي لما بقي منها.
5. دعم الحكومة بالموارد المالية اللازمة لتنفيذ المشروعات المدرجة ضمن الإستراتيجية.

ورشة: مبادرة إصلاح السياسات الرقمية (موجز السياسات)

المقدمة

افتتحت الورشة بكلمة ترحيبية من إسراء البكوش، التي قدمت لمحة عن مبادرة "أنير"، وهي مبادرة ليبية تهدف إلى تعزيز الوعي الرقمي وتطوير السياسات الرقمية في ليبيا، ثم إنها استعرضت أبرز إنجازات المبادرة في العام الماضي، والتحديات التي تواجهها، وخططها المستقبلية، بمشاركة نخبة من الخبراء والمتخصصين في المجال الرقمي.

مداخلة السيد/ أسامة منصور (عبر منصة zoom) هو أحد الخبراء الرئيسيين في مبادرة "أنير"، قدم عرضًا تفصيليًّا عن الإطار المنهجي لعملها.

أبرز النقاط في مداخلته

توضيح المفاهيم: فرّق بين المستويات التشريعية المختلفة:

- القوانين (التي تصدر عن الجهات التشريعية).
- الإستراتيجيات (التي تضع رؤية عامة وتمنع التكرار).
- والسياسات (الإجراءات التنفيذية).

طبيعة سياسات مبادرة أنير

أكد السيد/ أسامة منصور أن المبادرة لا تصدر سياسات بالمعنى الحكومي الملزم، بل تقدم موجزات سياسات، وهي وثائق استرشادية مبنية على أسس علمية وبحثية، تهدف إلى مساعدة صانعي القرار.

المخرجات الرئيسية

ثلاث موجزات سياسات:

- الأمن السيبراني.
- حماية البيانات الشخصية.
- الحيز الرقمي وحقوق الإنسان.

هذه الموجزات هي إطارات توجيهية واسترشادية مبنية على أسس علمية ومشاورات واسعة.

سياسة الخصوصية الاسترشادية

صممت خصيصًا للقطاع الخاص؛ لتكون خطوة استباقية لحماية بيانات المستخدمين في ظل غياب قانون وطني واضح.

مخرجات المبادرة

- **ورقة سياسات مقترحة:** أعدت ورقة سياسات مقترحة تتضمن توصيات لتطوير الإطار القانوني للقطاع الرقمي في ليبيا .
- **بوابة رقمية للسياسات:** أطلقت المبادرة بوابة رقمية تتيح للجميع المشاركة في اقتراح السياسات الرقمية ومناقشتها.
- مدرسة ليبيا لحوكمة الإنترنت: أطلقت نسخة 2025م من مدرسة ليبيا لحوكمة الإنترنت، وهي تهدف إلى تزويد الشباب والمهتمين بالأدوات اللازمة لفهم السياسات الرقمية وتطويرها.

التحديات

- عدم الاستقرار السياسي والأمني في ليبيا.
- تضارب الصلاحيات بين المؤسسات الحكومية .
- نقص الكوادر المتخصصة في المجال الرقمي.
- التحديات الأمنية والتهديدات المتزايدة.
- غياب التناغم بين المؤسسات.
- غياب الأطر القانونية الحديثة والاعتماد على قوانين قديمة لا تلائم التطور الرقمي.

النقاش ومداخلات الحضور

مداخلة د. عبد الرؤوف القصبي، رئيس جامعة السرايا الحمراء: أثنى المتحدث على المبادرة واقترح ضرورة زيارة الجامعات (العامة والخاصة) لتعريف الطلاب بهذه المفاهيم، لا سيما

مع وجود تخصصات حديثة مثل الأمن السيبراني والذكاء الاصطناعي، وأكد على أهمية تنظيم ورش وبرامج تدريب عملي للطلاب.

مداخلة عن التسمية والشمولية: تساءل أحد الحضور عن سبب حصر اسم المبادرة في "السياسات" بدلًا من "الإصلاح الرقمي" لتكون أكثر شمولية، مشيرًا إلى أن الإصلاح يتطلب توازنًا بين تطوير الخدمات من الأسفل وإصلاح القوانين من الأعلى.

أوضح فريق المبادرة أن اختيار مصطلح "السياسات" كان مدروسًا لتجنب الصدام مع الجهات الحكومية، إذ إن "الإصلاح" قد يُفهم على أنه تدخل في عمل الحكومة، أمّا المبادرة من جهة تابعة للمجتمع المدني فتقدم "مقترحات سياسات" يمكن للجهات الرسمية اعتمادها.

أهمية التوعية العامة

- أشار أحد المشاركين إلى أن الجمهور العام قد لا يهتم بقراءة السياسات المطولة، واقترح ضرورة تبسيط المحتوى وتقديمه في صور سهلة الوصول، مثل مقاطع الفيديو القصيرة باللغة العامية لنشر الثقافة الرقمية.

توحيد المصطلحات

- أكدت هذ المداخلة على أهمية توحيد المصطلحات في المجال الرقمي لتجنب سوء الفهم بين مختلف القطاعات (القانوني - التقني - الصحي - ...إلخ).

التوصيات

1. **توسيع نطاق المبادرة:** ضرورة توسيع نطاق عمل المبادرة لتشمل مدنًا وجامعات أخرى خارج طرابلس لزيادة الوعي والتأثير.
2. **التعاون الأكاديمي:** بناء شراكات مع الجامعات والمؤسسات التعليمية لتوعية الجيل الجديد وإعداد كوادر متخصصة.
3. **تبسيط المحتوى:** إنتاج محتوى توعوي مبسط (مثل فيديوهات قصيرة ورسوم بيانية) موجه للجمهور العام؛ لرفع مستوى الوعي بالحقوق والأمن الرقمي.

4. **بوابة السياسات الرقمية:** الاستفادة من البوابة الرقمية التي أطلقتها المبادرة كمنصة مفتوحة للجميع؛ لتقديم مقترحات سياسات والحصول على استشارات بشأنها.
5. **السعي نحو التوطين والسيادة الرقمية:** ضرورة العمل على مستوى إقليمي لتوطين التقنيات وإنشاء إطار عربي مشترك لحماية البيانات وتحقيق سيادة رقمية.
6. **تمكين وإشراك المجتمع المدني** :تعزيز دور منظمات المجتمع المدني وإشراكها في النقاشات وصنع السياسات؛ بما يضمن وصول أوسع وشمولية أكبر في الحوكمة الرقمية.

ورشة: مشروع قانون الجرائم الإلكترونية والدليل الرقمي

مقدمة

عُقدت الورشة لمناقشة مسودة مشروع قانون جديد يتعلق بـ"الجرائم الافتراضية والدليل الرقمي" في ليبيا. هدفت الجلسة إلى عرض نسخة شبه منقحة من القانون، وفتح باب النقاش حولها لجمع الملاحظات من مختلف الخبراء والمختصين، بما في ذلك ممثلين عن الهيئات القضائية، والمجتمع المدني، والجهات التقنية، والأمنية.

خلفية تاريخية

أوضحت الورشة أن العمل على هذا القانون ليس جديدًا؛ فقد بدأت المحاولات الأولى في عام 2008م، وقُدمت مسودات سابقة في 2009م و2015م، لكنها لم تكتمل، والنسخة الحالية هي محاولة جديدة ومحدثة تأخذ في الاعتبار التطورات التقنية والتشريعية.

الجهد البحثي

قبل صياغة المسودة، راجعت الجهة المسؤولة (إدارة مكافحة جرائم تقنية المعلومات) قوانين 22 دولة عربية، مع الإشارة إلى أن أحدثها هو القانون السوري الصادر في 2023م.

المواءمة الدولية

جرى الاطلاع على الاتفاقيات الدولية والإقليمية ذات الصلة، مثل "اتفاقية بودابست" المتعلقة بالجرائم السيبرانية، و"الاتفاقية العربية لمكافحة جرائم تقنية المعلومات"، إضافة إلى المعاهدات المتعلقة بحقوق الإنسان؛ لضمان التوازن في القانون.

كلمة الجمعية الليبية لأعضاء الهيئات القضائية

ألقى ممثل عن الجمعية كلمة رسمية أكد فيها على النقاط التالية:

- **الأهمية البالغة للقانون:** أثنى على المبادرة، مشيرًا إلى أن الورشة تأتي في وقت حاسم نظرًا للتصاعد المتسارع في وتيرة الجرائم المرتكبة في الفضاء الإلكتروني، فقد صارت هذه الجرائم تهديدًا حقيقيًّا للأمن القومي والمجتمعي.
- **أنواع الجرائم المستهدفة:** ذكر أمثلة عن الجرائم التي يجب أن يغطيها القانون، مثل اختراق الأنظمة، وانتهاك الخصوصية، والاحتيال، والابتزاز، والتشهير، ونشر الفكر المتطرف.
- **الدليل الرقمي:** شدد على أن الدليل الرقمي بات "حجر الزاوية" في إثبات هذه الجرائم، ما يستدعي وضع آليات دقيقة لحفظه وتحليله، واعتماده وسيلة قانونية موثوقة.
- **عرض الدعم والتعاون:** أعلنت الجمعية عن استعدادها الكامل لدعم المشروع بتقديم الاستشارات والمقترحات القانونية، وتوفير نخبة من القضاة ووكلاء النيابة ذوي الخبرة للمساهمة في صياغة قانون عصري ومتوازن.

مبررات المسودة الجديدة ومحتوياتها (عرض من إدارة مكافحة الجرائم)

- **الفجوة بين القانون والتطبيق:** أوضح المتحدث أن قانون رقم 5 السابق كان به قصور، وأن بين النصوص القانونية الجامدة والوقائع العملية التي تواجههم فجوة كبيرة، فالعديد من الجرائم الحديثة ليس لها تكييف قانوني واضح.
- **مواكبة التطورات:** المسودة الجديدة تهدف لسد هذه الفجوة ومواكبة التطورات التقنية مثل الذكاء الاصطناعي، وأساليب الجريمة الجديدة كتغليف البطاقات المصرفية (Skimming).
- **إحصائيات مقلقة:** عُرضت إحصائيات تظهر ارتفاعًا كبيرًا في معدلات الجرائم الإلكترونية، فقد سُجّلت 470 قضية في النصف الأول من عام 2025م، ومن المتوقع أن تصل إلى أكثر من 900 قضية بنهاية العام، مقارنة بـ 604 قضايا في 2024م.
- **مواد جديدة وجرائم أضيفت:** المسودة الجديدة تعالج أفعالًا لم تكن مجرّمة بوضوح في السابق، منها:

إساءة استخدام التشفير لأغراض إجرامية

- إرسال البريد الإلكتروني الدعائي غير المرغوب فيه (Spam).
- نشر الأخبار الكاذبة والشائعات.
- حيازة الوسائط التقنية المحظورة.
- الترويج الرقمي للمخدرات.
- المراهنات والقمار الرقمي.
- التحريض الرقمي.
- المسؤولية القانونية لمقدمي خدمة استضافة المحتوى المحظور.

النقاشات والملاحظات الرئيسية

ملاحظات قانونية هيكلية (قدمها د. محمد)

- **تسمية القانون:** اقترح تغيير اسم القانون من "الجرائم الافتراضية" إلى "الجرائم الإلكترونية"، لأن مصطلح "الافتراضية" لا يستوعب كل أبعاد الجريمة، أما "الإلكترونية" هو المصطلح الأوسع والأكثر اعتمادًا دوليًا.
- **الدليل الرقمي:** انتقد فكرة إدراج "الدليل الرقمي" في عنوان القانون، موضحًا أنه أثر من آثار الجريمة ويجب تنظيم أحكامه ضمن "قانون الإجراءات الجنائية" وليس في قانون عقابي موضوعي.
- **صياغة النصوص:** أشار إلى أن نصوص المسودة طويلة ومفصلة بإسهاب مبالغ فيه، والقوانين العقابية يجب أن تكون موجزة وتضع قواعد عامة، وتترك التفاصيل للوائح التنفيذية لتسهيل تحديثها مع تغير التقنية.
- **مسؤولية الشخص الاعتباري (الشركات والمؤسسات):** انتقد القانون لعدم معالجته مسؤولية الكيانات بصورة كافية، فمن رأيه يجب أن تكون المؤسسة مسؤولة جنائيًا عن الجرائم التي يرتكبها موظفوها لصالحها.

الوضع القانوني للقرصنة الأخلاقية (Ethical Hacking)

استفسرت إحدى الحاضرات عن الإطار القانوني الذي يحمي "الهكر الأخلاقي" الذي توظفه شركة خاصة لاختبار أمن أنظمتها.

- **الرد:**
  - أوضح المتحدثون أن هذا المجال يعمل حاليًّا في "منطقة رمادية" قانونيًّا.
  - جرت الإشارة إلى أن المادة 14 من المسودة قد تعالج هذا الأمر، فهي تعفي من العقوبة من ينفذ هذه الأفعال بحسن نية لأغراض الاختبارات الفنية المشروعة أو للحماية.
  - كان الاتفاق على ضرورة وجود آلية واضحة لمنح التراخيص والتصاريح لهذه المهنة لتوفير غطاء قانوني وحماية لجميع الأطراف.

مخاوف بشأن حرية الرأي والتعبير (قدمها أ. رامي من مجتمع الإنترنت)

- **وصف القانون بـ"القمعي":** أبدى قلقه من أن بعض مواد القانون، مثل المادة 39 المتعلقة بالتشهير، قد تستخدم "عصا" لقمع حرية الرأي والتعبير، خاصة ضد الصحفيين والنشطاء.
- **التمييز بين الإعلام والأفراد:** انتقد التفريق في العقوبة بين وسائل الإعلام المسجلة والأفراد على وسائل التواصل الاجتماعي، لأن هذا يضع المواطن العادي تحت طائلة عقوبات أشد.
- **الحل المقترح:** طالب بأن تكون القضايا المتعلقة بالتشهير "مدنية" (تقتصر على التعويض المالي) وليست "جنائية" (تؤدي إلى السجن).
- **الرد على المخاوف:** رد مقدم الورشة بأن القانون يفرق بين "النقد المهني للصفة الوظيفية" (وهو أمر مشروع) و"التشهير والسب الشخصي" (وهو جريمة)، وقال إن المشكلة ليست في القانون بقدر ما هي في ثقافة المجتمع التي تخلط بين الأمرين.

مقترح للتنسيق مع الجهات التشريعية الأخرى (قدمه د. مجدي)

اقترح ضرورة التنسيق مع "مركز البحوث القانونية والقضائية" الذي يعمل حاليًّا على تعديل شامل لـ "قانون العقوبات" و"قانون الإجراءات الجنائية"؛ لضمان دمج أحكام الجرائم الإلكترونية على نحو متكامل وتجنب تضارب التشريعات.

المسؤولية القانونية في عصر الذكاء الاصطناعي

- **طُرِحَ تساؤل مهم عن المسؤولية الجنائية في حال ارتكبت آلة تعمل بالذكاء الاصطناعي (مثل سيارة ذاتية القيادة) جريمةً أو تسببت في حادث.**

النقاش: من المسؤول؟ المبرمج؟ الشركة المصنعة؟ أم مالك الآلة؟

التوجه العالمي: جرى توضيح أن هذا الموضوع لا يزال نقطة بحث عالمية ساخنة، وأن التوجه الحالي يميل نحو فرض ما يسمى بـ (Human in the loop) أي وجود إنسان في حلقة التحكم، بمعنى اشتراط وجود إشراف بشري على قرارات الآلة لتحميل هذا الشخص المسؤولية القانونية.

الخلاصة والمخرجات

1. **المسودة ليست نهائية:** جرى التأكيد مرارًا على أن هذه الورشة هي خطوة أولى، وأن المسودة المعروضة قابلة للنقد والتعديل، وستُؤخذ جميع الملاحظات بعين الاعتبار.
2. **أهمية التنسيق:** توجد حاجة ماسة للتنسيق بين مختلف الجهات (الأمنية، والقضائية، والتشريعية، ومراكز البحوث) لإنتاج قانون متكامل وفعّال.
3. **تحديات رئيسية:** برزت تحديات جوهرية تتعلق بضرورة الموازنة بين مكافحة الجريمة وحماية حقوق الإنسان وحرية التعبير، إضافة إلى التحديات القانونية التي يفرضها التطور التقني السريع مثل الذكاء الاصطناعي.
4. **دعوة مفتوحة للمشاركة:** وجّهت دعوة للحاضرين وللخبراء الآخرين لتقديم ملاحظاتهم المكتوبة للمساهمة في تحسين المسودة.

ورشة: لائحة حماية البيانات الشخصية الصادرة عن مصرف ليبيا المركزي

الجهة المنظمة

- إدارة البحوث والإحصاء - مصرف ليبيا المركزي.

المتحدث الرئيسي

- المستشار ربيع الراقوبي، مستشار في مصرف ليبيا المركزي وأحد أعضاء اللجنة الفنية التي أعدت اللائحة.

المقدمة

عُقدت هذه الورشة بهدف تسليط الضوء على "نظام حماية البيانات واللائحة التنظيمية" التي أصدرها مصرف ليبيا المركزي بموجب المنشور رقم 18 بتاريخ 1 يونيو 2025م.

استهل المستشار ربيع الراقوبي الجلسة بتقديم شكره للجهة المنظمة، موضحًا أن الهدف من اللائحة هو خلق أساس تشريعي وتنظيمي واضح لحماية البيانات داخل القطاع المصرفي والمالي في ليبيا، نظرًا لغياب مرجعية قانونية محددة في هذا الشأن سابقًا.

أشار المستشار إلى أن إعداد اللائحة استغرق قرابة ستة أشهر من العمل المكثف من قبل لجنة متخصصة، واجهت فيها تحديات متعددة لصياغة إطار عمل يناسب واقع القطاع المالي في ليبيا. وأكد أن الجلسة ستكون حوارية وتفاعلية للإجابة عن استفسارات الحضور وتوضيح أي غموض حول بنود اللائحة.

محاور الورشة

المحور الأول: الإطار العام للائحة وأهدافها

أوضح المستشار ربيع الروبي أن النظام يهدف إلى تنظيم عملية التعامل مع البيانات بجميع أنواعها داخل المؤسسات المالية، ويشمل ذلك:

- **البيانات الشخصية:** معلومات تعريفية خاصة بالأفراد.
- **البيانات المالية والائتمانية:** تفاصيل الحسابات والمعاملات والتاريخ الائتماني.
- البيانات الحساسة: أي معلومات أخرى تتطلب درجة عالية من السرية.

تُغطي اللائحة دورة حياة البيانات برمتها، بدءًا من أحقية الجمع، مرورًا بالمعالجة، والتخزين، ومدة الاحتفاظ، وإجراءات الحماية، وانتهاءً بآلية الإزالة الآمنة للبيانات.

المحور الثاني: نطاق التطبيق والجدول الزمني الإلزامي

جرى التأكيد على أن اللائحة ستكون نافذة وملزمة لجميع المؤسسات الخاضعة لرقابة مصرف ليبيا المركزي، اعتبارًا من تاريخ 1 يوليو 2026م، وتشكل هذه المؤسسات:

- مصرف ليبيا المركزي والمصارف التجارية.
- فروع المصارف الأجنبية العاملة في ليبيا.
- شركات التكنولوجيا المالية (FinTech).

- شركات خدمات الدفع الإلكتروني.
- شركات الصرافة.
- المؤسسات والشركات التي تقدم خدمات ائتمانية.
- شركات التأجير التمويلي.

المحور الثالث: سيادة البيانات والتخزين داخل ليبيا (النقطة الأكثر جدلًا)

كان هذا المحور نقطة النقاش الأبرز في الورشة، فقد نصت اللائحة بصورة قاطعة على "عدم جواز تخزين البيانات الشخصية، أو المالية، أو الائتمانية، أو الحساسة خارج حدود الدولة الليبية".

أثار الحضور تساؤلات حول إمكانية استخدام خدمات الحوسبة السحابية (Cloud) العالمية أو تخزين نسخ احتياطية مشفرة في الخارج.

- **الرد:** كان رد المستشار حاسمًا بأن التخزين يجب أن يكون داخل ليبيا بنسبة 100%. وأوضح أن المصرف المركزي أجرى مسحًا للسوق المحلي، وتأكد من وجود سعة كافية لدى مزودي الخدمات المحليين (مراكز البيانات) لتغطية احتياجات القطاع المالي كله، مع وجود قابلية للتوسع مستقبلًا. يمكن للمؤسسات بناء مراكز بيانات خاصة بها أو الاستعانة بخدمات الاستضافة من شركات ليبية متخصصة.

المحور الرابع: العقوبات والمخالفات

أوضح المستشار أن اللائحة تتضمن عقوبات رادعة لضمان الامتثال، وأهمها:

- غرامة مالية قدرها 100,000 دينار ليبي عن كل مخالفة. وجرى التشديد على أن هذه القيمة تُطبق على "كل مخالفة على حدة" وليست غرامة إجمالية، ما يعني أن تكرار المخالفات لعدد كبير من العملاء قد يؤدي إلى غرامات مليونية.
- إمكانية سحب الترخيص لبعض أنواع الشركات (مثل شركات التكنولوجيا المالية) في حال تكرار المخالفات الجسيمة.
- فتح الباب أمام أي عقوبات أخرى يراها مصرف ليبيا المركزي مناسبة.

المحور الخامس: تحديات البنية التحتية والكفاءات المحلية

أعرب بعض الحضور عن قلقهم من ضعف البنية التحتية التقنية في ليبيا وعدم قدرتها على مجاراة المعايير العالمية، إضافة إلى الاعتماد الحالي على شركات أجنبية وخبرات أجنبية.

- **الرد:** فنّد المستشار فكرة غياب الكفاءات المحلية، مشيرًا إلى وجود شركات ليبية قادرة على تقديم خدمات استضافة ومراكز بيانات بمعايير عالية (وذكر بعضها بالاسم من بين الحضور)، وأكد أن وجود اللائحة سيخلق طلبًا في السوق المحلي، ما سيشجع هذه الشركات على تطوير خدماتها. ثم إنه أشار إلى أن المصرف المركزي بصدد تنظيم قائمة بالشركات التقنية المعتمدة لتقديم الخدمات للقطاع المالي.

المحور السادس: استخدام البيانات والموافقة الصريحة للعميل

نوقش موضوع استخدام بيانات العملاء لأغراض تسويقية. وأكدت اللائحة على ضرورة الحصول على "موافقة صريحة ومسبقة" من العميل قبل استخدام بياناته لأي غرض ثانوي غير الخدمة الأساسية المقدمة له، على أن تكون الموافقة اختيارية وليست شرطًا إلزاميًّا للحصول على الخدمة.

المحور السابع: المسؤولية القانونية وتعيين "مسؤول البيانات"

لتجاوز مشكلة التنسيق البطيء بين الإدارات، نصّت اللائحة على ضرورة تعيين منصب جديد داخل كل مؤسسة مالية وهو (مسؤول البيانات Data Officer).

- **مهامه:** يكون هذا الشخص (ويُشترط أن يكون ليبي الجنسية) مسؤولًا مباشرًا عن الإشراف على تطبيق اللائحة، والتنسيق بين جميع الإدارات، ويكون حلقة الوصل مع مصرف ليبيا المركزي.
- **المساءلة:** يتحمل مسؤول البيانات المسؤولية المباشرة في حال وجود تقصير في تطبيق بنود اللائحة.

التوصيات

كانت الورشة منصة مهمة لتوضيح الأبعاد التنظيمية والقانونية للائحة حماية البيانات، التي تمثل نقلة نوعية في تنظيم القطاع المالي في ليبيا. ويمكن تلخيص المخرجات في النقاط التالية:

1. **الإلزامية المطلقة:** اللائحة ستكون ملزمة إلزامًا كاملًا بحلول 1 يوليو 2026م، ولا مجال للتأجيل.
2. **سيادة البيانات:** مبدأ تخزين البيانات داخل ليبيا هو حجر الزاوية في اللائحة، وهو غير قابل للتفاوض.
3. **المسؤولية المشتركة:** تقع المسؤولية على عاتق المؤسسة المالية كلها، مع تحديد مسؤول مباشر متمثل في (مسؤول البيانات).
4. **الجانب الرادع:** العقوبات المالية مصممة لتكون رادعة وتُحتسب على أساس كل مخالفة، ما يجعل عدم الامتثال خيارًا مكلفًا للغاية.

التوصية الأهم للمؤسسات المالية هي البدء فورًا بوضع خطط عمل واضحة للامتثال للائحة في المهلة الممنوحة، وتقييم بنيتها التحتية الحالية، واستكشاف الشراكات مع مزودي الخدمات المحليين؛ لتلبية متطلبات التخزين والمعالجة داخل ليبيا.

الخاتمة

كان منتدى حوكمة المعلوماتية 2025م محطة مهمة جمعت مختلف الأطراف المعنية، من خبراء وأكاديميين، وممثلين عن المؤسسات الحكومية والخاصة، ومنظمات المجتمع المدني، بهدف مناقشة واقع حوكمة المعلوماتية في ليبيا واستشراف آفاقها المستقبلية. وقد أتاح المنتدى مساحة للحوار وتبادل الرؤى حول التحديات والفرص، وأكد على أهمية تعزيز البنية المؤسسية والتشريعية والتقنية لمواكبة التحول الرقمي.

إن هذه المخرجات ستكون قاعدة عملية يمكن البناء عليها؛ لتطوير سياسات وطنية وإستراتيجيات أكثر تكاملًا وفاعلية في مجال حوكمة المعلوماتية.

التوصيات

1. **إعداد إطار وطني شامل لحوكمة المعلوماتية** يحدد الأدوار والمسؤوليات بين المؤسسات المختلفة ويضمن التنسيق الفعّال فيما بينها.
2. **تعزيز البنية التشريعية والتنظيمية** بتحديث القوانين ذات العلاقة بالبيانات والخصوصية والأمن السيبراني.
3. **إنشاء منصات وطنية للتشاور والتنسيق الدوري** تجمع الجهات الحكومية والقطاع الخاص والأكاديميين ومنظمات المجتمع المدني.
4. **تطوير القدرات البشرية** عن طريق برامج تدريبية متخصصة تستهدف الكوادر في المؤسسات الحكومية والخاصة.
5. **تشجيع الشراكات الدولية والإقليمية** للاستفادة من التجارب الناجحة في مجال الحوكمة الرقمية والأمن السيبراني.
6. **إطلاق مبادرات توعوية ومجتمعية** لتعزيز الثقافة الرقمية لدى الأفراد والجهات المختلفة، وزيادة الوعي بأهمية الحوكمة.
7. **دعم البحث العلمي والابتكار التقني** في الجامعات والمراكز البحثية، وربطه بالاحتياجات الوطنية في مجال حوكمة المعلوماتية.

فهرس المصطلحات

1. **التحول الرقمي(Digital Transformation) :** هو عملية شاملة لدمج التقنيات الرقمية في جميع جوانب الأعمال والعمليات الحكومية والمجتمعية، مما يؤدي إلى تغييرات جوهرية في الثقافة والعمليات ونماذج الأعمال؛ لتقديم قيمة جديدة وتحسين تجربة المستخدم.

2. **الأمن السيبراني(Cybersecurity) :** هو مجموعة التقنيات والعمليات والضوابط المصممة لحماية الأنظمة والشبكات والبرامج والبيانات من الهجمات الرقمية والتلف، أو الوصول غير المصرح به أو التعديل أو التعطيل.

3. **الذكاء الاصطناعي(AI - Artificial Intelligence) :** هو أحد فروع علوم الحاسوب، يهدف إلى تطوير أنظمة وبرامج قادرة على محاكاة القدرات الذهنية البشرية، مثل: التعلم والفهم، وحل المشكلات واتخاذ القرارات، وإدراك البيئة والاستجابة لها.

4. **النطاق الوطني (ccTLD - Country Code Top-Level Domain):** هو جزء من اسم النطاق (Domain Name)على الإنترنت، يتكون من حرفين ويمثل رمزًا لدولة أو منطقة جغرافية معينة، مثل ".ly" لليبيا، ويُستخدم لتمييز الوجود الرقمي للدولة.

5. **السيادة الرقمية(Digital Sovereignty) :** هي قدرة الدولة على التحكم في بنيتها التحتية الرقمية وبياناتها ومعلوماتها، وصياغة قوانينها وسياساتها الرقمية الخاصة، وحماية مواطنيها ومؤسساتها في الفضاء الإلكتروني، دون تدخل خارجي غير مبرر.

6. **حماية البيانات الشخصية(Personal Data Protection) :** هي مجموعة من القوانين واللوائح والإجراءات، التي تهدف إلى حماية خصوصية الأفراد فيما يتعلق بجمع بياناتهم الشخصية ومعالجتها وتخزينها ومشاركتها، وضمان استخدامها بطريقة عادلة وشفافة وآمنة.

7. **الجرائم الإلكترونية(Cybercrimes - Electronic Crimes) :** هي أي فعل غير قانوني يكون باستخدام الحاسوب أو شبكة الإنترنت أو جهاز إلكتروني يكون أداة رئيسية أو هدفًا للجريمة، وتشمل: الاختراق، والاحتيال الإلكتروني، والابتزاز الرقمي، ونشر المحتوى غير القانوني.

8. **التأمين السيبراني(Cyber Insurance) :** هو نوع من وثائق التأمين، يهدف إلى حماية الشركات والمؤسسات من الخسائر المالية الناجمة عن الهجمات السيبرانية واختراق البيانات وغيرها من الحوادث الرقمية، ويغطي عادة تكلفة الاستجابة للحوادث، واستعادة البيانات، والمسؤولية القانونية.

9. **البنية التحتية الحيوية(Critical Infrastructure) :** هي الأنظمة والموارد (المادية والرقمية) التي تُعد أساسية لعمل المجتمع واقتصاده، وهي التي قد يؤدي تعطيلها أو تدميرها إلى آثار سلبية خطيرة على الأمن القومي، أو السلامة العامة، أو الصحة، أو الاقتصاد، مثل: شبكات الاتصالات، والطاقة، والمياه، والقطاع المالي.

10. **هجوم الحرمان من الخدمة(DDoS - Distributed Denial of Service attack) :** هو نوع من الهجمات السيبرانية التي تهدف إلى تعطيل وصول المستخدمين الشرعيين إلى خدمة أو موقع إلكتروني، عن طريق إغراق الخوادم بكم هائل من طلبات الاتصال المزيفة القادمة من مصادر متعددة وموزعة.

11. **التصيد الاحتيالي(Phishing) :** هو محاولة احتيالية للحصول على معلومات حساسة (مثل: أسماء المستخدمين، وكلمات المرور، وبيانات البطاقات الائتمانية)، عن طريق انتحال شخصية جهة موثوقة (مثل بنك أو شركة معروفة) في رسالة إلكترونية أو رسالة نصية أو صفحة ويب مزيفة.

12. **الهندسة الاجتماعية(Social Engineering) :** هي فن التلاعب بالأفراد وخداعهم للحصول منهم على معلومات سرية، أو لإجبارهم على فعل أشياء معينة، بدلًا من استخدام الثغرات التقنية، وتعتمد على استغلال نقاط الضعف البشرية والثقة.

13. **نماذج مفتوحة المصدر(Open-Source Models) :** هي نماذج برمجية أو خوارزميات (خاصة في مجال الذكاء الاصطناعي) تكون شيفرتها المصدرية متاحة للجمهور، مما يسمح لأي شخص بالاطلاع عليها وتعديلها وتوزيعها، وتشجع على التعاون والابتكار المجتمعي.

14. **معالجة اللغة الطبيعية(NLP - Natural Language Processing) :** هو أحد فروع الذكاء الاصطناعي يركز على تمكين أجهزة الحاسوب من فهم اللغة البشرية وتفسيرها وتوليدها والتفاعل مع بطريقة ذات معنى، ما يتيح تطبيقات مثل الترجمة الآلية ومساعدي الذكاء الاصطناعي.

15. **الهوية الرقمية(Digital Identity) :** هي مجموعة من السمات والخصائص الإلكترونية التي تميز فردًا أو كيانًا في الفضاء الرقمي، وتستخدم للمصادقة على الهوية عند الوصول إلى الخدمات أو الأنظمة الرقمية.

16. **إمكانية الوصول الرقمي(Digital Accessibility) :** تعني تصميم المنتجات والخدمات الرقمية وتطويرها (مثل المواقع الإلكترونية والتطبيقات) بما يمكن الأشخاص ذوي الإعاقة وكبار السن من استخدامها والوصول إليها والتعامل معها بفاعلية وسهولة.

17. **إنترنت الأشياء(IoT - Internet of Things) :** هو مفهوم يشير إلى شبكة من الأجهزة المادية المتصلة بالإنترنت، والمزودة بأجهزة استشعار وبرامج وتقنيات أخرى تسمح لها بجمع البيانات وتبادلها مع أنظمة أخرى عبر الإنترنت.

18. **الحوسبة السحابية(Cloud Computing) :** هي نموذج لتقديم الخدمات الحاسوبية (مثل: الخوادم، والتخزين، وقواعد البيانات، والبرمجيات، والشبكات، والتحليلات) عبر الإنترنت (السحابة)، ما يسمح بالوصول إليها عند الطلب، ودون الحاجة إلى امتلاك بنية تحتية مادية.

19. **مراكز البيانات (Data Centers):** هي منشآت مادية ضخمة تحتوي آلافًا من الخوادم ومعدات الشبكات وأنظمة التخزين والبنية التحتية الداعمة (مثل أنظمة التبريد والطاقة)، وتُستخدم لتخزين كميات هائلة من البيانات ومعالجتها وتوزيعها.

20. **التكنولوجيا المالية(FinTech - Financial Technology) :** هو مصطلح يشير إلى استخدام التكنولوجيا والابتكار لتحسين الخدمات المالية أو أتمتتها، وتضم شركات تقدم حلولًا في المدفوعات الرقمية، والإقراض عبر الإنترنت، والاستثمار الآلي، وغيرها.

21. **مسؤول البيانات(Data Officer) :** هو منصب في المؤسسة مسؤول عن الإشراف على حوكمة البيانات، وضمان الامتثال للوائح حماية البيانات، وتطوير سياسات إدارة البيانات وتنفيذها، ويكون حلقة الوصل الرئيسية مع الجهات الرقابية.

22. **القرصنة الأخلاقية(Ethical Hacking) :** هي عملية اختراق نظام حاسوبي أو شبكة بشكل قانوني ومصرح به من قبل مالك النظام، بهدف تحديد نقاط الضعف الأمنية ومعالجتها قبل أن يستغلها المتسللون الخبيثون.

23. **الامتثال(Compliance) :** هو الالتزام بالقوانين واللوائح والمعايير والسياسات الداخلية والخارجية التي تنطبق على عمل المؤسسة، ويشمل ذلك جوانب مثل حماية البيانات، والأمن السيبراني، والمعايير التشغيلية.

24. **التوفر(Availability) :** (في سياق أمن المعلومات) هو ضمان أن الأنظمة والبيانات والخدمات يمكن أن يستخدمها المستخدمون المصرح لهم عند الحاجة، وأن يصلوا إليها دون انقطاع أو تأخير.

25. **السرية(Confidentiality) :** (في سياق أمن المعلومات) هو ضمان حماية المعلومات من الوصول غير المصرح به أو الكشف عنها، والحفاظ على خصوصية البيانات وعدم إفشائها إلا للأطراف المخولين بذلك.

26. **النزاهة(Integrity) :** (في سياق أمن المعلومات) هو ضمان دقة المعلومات والأنظمة واكتمالها وموثوقيتها، وحمايتها من التعديل أو التلف غير المصرح به، ما يضمن أن البيانات لم تُغير بطريقة غير مصرح بها.

27. **الهيئة الوطنية لأمن وسلامة المعلومات (NISSA - National Information Security and Safety Authority):** الهيئة الوطنية لأمن وسلامة المعلومات هي الجهة الحكومية الرسمية في ليبيا المسؤولة عن حماية نظم المعلومات والاتصالات وتأمينها على مستوى الدولة، تأسست سنة 2013م، وهي تعمل على تطوير السياسات الوطنية للأمن السيبراني، ومراقبة التهديدات الرقمية والاستجابة لها.

28. **المؤسسة الليبية للتقنية(Libyan Technology Foundation) :** هي مؤسسة مجتمع مدني غير ربحية غير حكومية تشارك بفاعلية في المشاريع والحوارات الحكومية والمجتمعية؛ لتعزيز التحوّل والحوكمة الرقمية، وتطوير التشريعات الخاصة بقطاع تقنية المعلومات والاتصالات في ليبيا.

29. **الهيئة العامة للاتصالات والمعلوماتية (General Authority for Communications and Informatics):** هي جهة حكومية ليبية تتولى مسؤولية تنظيم قطاع الاتصالات والمعلوماتية في ليبيا، وتحديد السياسات والتشريعات المتعلقة بهذا القطاع.

30. **مصرف ليبيا المركزي(Central Bank of Libya) :** هو المؤسسة المالية السيادية في ليبيا، المسؤولة عن السياسة النقدية وإصدار العملة والإشراف على القطاع المصرفي والمالي في البلاد.

31. **مجتمع الإنترنت - ليبيا(ISOC Libya Chapter) :** هو فرع محلي لمنظمة مجتمع الإنترنت العالمية(Internet Society) ، يعمل على تعزيز تطوير الإنترنت واستخدامه المفتوح والآمن في ليبيا، ويدعم قضايا حوكمة الإنترنت.

32. **Community Based MAG:** مصطلح يشير إلى مجموعة استشارية متعددة من أصحاب المصلحة (Multi-stakeholder Advisory Group) قائمة على المجتمع، تعمل على تسهيل نقاشات حوكمة الإنترنت من منظور مجتمعي وشامل.

33. **LibyaCERT: هو** الفريق الوطني للاستجابة لطوارئ الحاسوب والشبكات في ليبيا (Libyan Computer Emergency Response Team) ، وهو مسؤول عن الاستجابة للحوادث الأمنية السيبرانية على المستوى الوطني.

34. **ISACA:** هي رابطة عالمية للمتخصصين في حوكمة تكنولوجيا المعلومات والأمن والتدقيق والمخاطر والامتثال، وتصدر إطارات عمل ومعايير مهنية في هذه المجالات.

35. **ISO/IEC 27001:** هو معيار دولي لنظام إدارة أمن المعلومات (ISMS - Information Security Management System) ، يحدد المتطلبات اللازمة لإنشاء نظام إدارة أمن المعلومات وتطبيقه وتشغيله ومراقبته ومراجعته وصيانته وتحسينه.

36. **SIEM (Security Information and Event Management):** هو نظام يجمع البيانات الأمنية من مصادر متعددة داخل الشبكة (مثل السجلات وأحداث الأمان) ، ويحللها في الوقت الفعلي للكشف عن التهديدات والأنماط المشبوهة.

37. **KaliGPT:** هو نموذج ذكاء اصطناعي (أو أداة مبنية على الذكاء الاصطناعي) مُصمم خصيصًا لمساعدة مختبري الاختراق (Penetration Testers) في مهامهم الأمنية.

38. **Blue Team Defender GPT:** هو نموذج ذكاء اصطناعي (أو أداة مبنية على الذكاء الاصطناعي) مُصمم لتعزيز قدرات فرق الدفاع السيبراني (Blue Team) في كشف التهديدات وتحليلها والاستجابة لها.

39. **Corden Pharma IBM Watson:** يشير إلى تعاون بين شركة الأدوية Corden Pharma ومنصة الذكاء الاصطناعيIBM Watson ، بهدف استخدام الذكاء الاصطناعي في مجالات مثل حماية البيانات الحساسة أو تحسين العمليات.