استشراف

مركز الدراسات الاستشرافية

PROSPECTIVE STUDIES CENTER

التطوّر الرقمي وحماية المعلومات

أصل هذا الكتاب

منتدى عقده مركز الدراسات الاستشرافية - عنْ بعد -

بتأريخ ٢١ جمادي الأولى ١٤٤٧ ، الموافق ١٢ نوفمبر ٢٠٢٥

وشارك فيه كل من

د.محمد بن عبدالرحمن العبدالكريم

عضو هيئة التدريس

بكلية علوم الحاسب والمعلومات بجامعة الملك سعود

د.عاصم بن ناصر اليحيى

عضو هيئة التدريس

بكلية علوم الحاسب والمعلومات بجامعة الملك سعود

مداخل رئيسي في المنتدى

أ.د .عبدالقادر بن عبدالله الفنتوخ

عضو هيئة التدريس بجامعة الملك سعود

و وكيل وزارة التعليم العالي للتخطيط والمعلومات سابقاً

مدير المنتدى

د.زياد بن عبدالله وكيل الشيخ

عضو هيئة التدريس

بكلية علوم الحاسب والمعلومات بجامعة الإمام

الفهرس


بسم الله الرحمن الرحيم

مقدمة:

يشهد العالم اليوم انعطافةً تاريخيةً غير مسبوقة؛ حيث لم يعد التحول الرقمي مجرد خيارٍ تقنيٍ تسعى إليه المؤسسات، بل أصبح ضرورةً وجوديةً ومحركاً أساسياً للاقتصاد العالمي والنمو الاجتماعي، ونحن نعيش في عصر «الثورة الصناعية الرابعة»، حيث تتداخل التقنيات المادية والرقمية والبيولوجية لتعيد صياغة مفهوم الواقع؛ من الذكاء الاصطناعي الذي يتنبأ باحتياجاتنا، إلى إنترنت الأشياء التي تربط مدننا، وصولاً إلى الحوسبة السحابية التي أزالت الحدود الجغرافية؛ كل هذه القفزات جعلت من البيانات «النفط الجديد» والمورد الأثمن في القرن الحادي والعشرين، ولكن، مع هذا الارتماء في حضن الرقمنة، برز تحدٍ موازٍ في حجمه وخطورته: حماية المعلومات؛ فبينما يفتح العالم الرقمي أبواباً واسعةً من الفرص والرفاهية، فإنه يفتح أيضاً ثغراتٍ قد ينفذ منها التهديد السيبراني الذي لا يعرف حدوداً.

وفي قلب هذا الحراك العالمي، تقف المملكة العربية السعودية كنموذجٍ رائدٍ واستثنائيٍ في سرعة ونوعية التحول الرقمي، ولم تكن الرقمنة في المملكة وليدة الصدفة، بل جاءت كثمرة لرؤية السعودية ٢٠٣٠، التي وضعت التحول الرقمي في صميم مستهدفاتها لبناء مجتمعٍ حيويٍ، واقتصادٍ مزدهرٍ، ووطنٍ طموح، لقد نجحت المملكة في تحويل مدنها إلى مدن ذكية وطورت بنيةً تحتيةً رقميةً هي الأكفأ في المنطقة؛ ممّا جعل الخدمات الحكومية –من خلال منصات مثل «أبشر» و«توكلنا»– معياراً عالمياً في الكفاءة والسهولة.

لقد أصبحت الهجمات الإلكترونية، وتسريب البيانات، والتجسس الرقمي من أكبر المخاطر التي تهدد استقرار الدول واقتصاداتها؛ لذا، بات مفهوم «الأمن السيبراني» هو الدرع الحامي لهذا التحول، والضمانة الوحيدة لاستمرارية الثقة بين الإنسان والآلة. إن العلاقة بين التطور الرقمي وحماية المعلومات هي علاقةٌ طرديةٌ؛ فكلما زاد اعتمادنا على التقنية، زادت الحاجة إلى أنظمة حمايةٍ أكثر ذكاءً وقدرةً على التكيف، والتحدي اليوم ليس تقنياً فحسب، بل هو تحدٍ بشريٌ وثقافيٌ يتمثّل في بناء وعيٍ جمعيٍ بأهمية أمن المعلومات.

المحور الأول

التحول الرقمي

إنّ ما نعيشه من «تقنية المعلومات والاتصالات»، وبعد ذلك أصبح «التحول الرقمي» هو تطورٌ، ولعلي أُذكّر بنظرية قديمة جداً، وهي أنّ الحاسبات تتضاعف سرعتها وتتضاعف، مصداقاً لقانون «مورسلو (Moore's Law)، وهو أن يكون هناك تضاعفٌ للتقنية كل ثمانية عشر شهراً تقريباً بنفس التكلفة، فما نراه الآن على أيامنا كان حُلماً بعيد التحقق، وهذا التطور دعا طبعاً إلى أن الجهات -أو على مستوى الدولة عموماً- يكون لها تغيرٌ في طريقة عمل تقنية المعلومات، وسابقاً كان الوصول إلى الأجهزة محدُوداً، ولا يستطيعه إلا أشخاص محدودون، أما الآن فلا؛ فقد أصبح من السهولة بمكان الوصول للتقنية والحصول عليها والعمل عليها، وأصبحت بسرعاتٍ عالية، وسعاتٍ كبيرة؛ وهذا بلا شك مكّن من التطور، إلا أنه أيضاً وفي نفس الوقت نشأ معها جيلٌ مُعتمدٌ، أو اعتاد على هذه التقنيات؛ فبطبيعة الحال فالتحول في مُسميات، أو إدارات تقنية المعلومات تحولٌ طبيعيٌ لما نلمسه حولنا من تطور في التقنيات.

وبالنسبة للتغير في العمل، لو عدنا أربع أو خمس سنوات للوراء وتذكرنا كورونا وكيف غيّرت في التعليم، وغيّرت في نموذج العمل، بل إنّ برنامج (زووم) الذي نستخدمه لم يحصل له الانتشار القوي إلا في تلك الفترة؛ فالاستعداد

التقني كان موجوداً، لكن الناس لم تكن مُقبلةً عليه، وظروف جائحة كورونا دفعت الناس للتعليم عن بعد ودفعتهم للعمل عن بعد؛ وبدأ الناس يتحولون فعلاً إلى نوع جديد من استخدامات الحاسب، أو التطبيقات، ومن الأشياء الرئيسية التي دفعت الناس، أو شجعت الناس هو تطور التطبيقات؛ مثال: أنظمة تحديد المواقع (GPS) التي ساهمت في تطوير تطبيقت في التوصيل ، التي جعلت الجيل الجديد يعتمد على هذه التطبيقات أكثر من أيّ شيء آخر، كل هذه الدوافع والعوامل دفعت الناس إلى أن يتحولوا إلى هذا المجال، أو إلى التحول الرقمي.

أثر التحوّل الرقمي في التعليم

قديماً لما قدّمنا على الجامعة كنا نأتي بملف أخضر، ونذهب لعمادة القبول والتسجيل ونعطيهم الملف، الآن أصبح التقديم عن بعد، والعام الماضي أصبح التقديم على جميع الجامعات في المملكة عن طريق منصة مُوحّدة، وما كان هذا سيحْصُل لولا وجود التطور الرقمي، والتطورات –هذه وخاصة إذا كانت مُتسارعة– لها تبعاتٌ بلا شك؛ وبعض الناس لمس أن هناك بعض الأخطاء، وهناك بعض التخوّف من النتائج، لكن في النهاية تظل التقنية مُستمرةً في التطور، ويبقى كيف نستفيد من هذه التقنية في مجال التعليم؛

فالآن أصبح استخدام التعلم الإلكتروني أمراً شبه ضروري، بل إنّ رفع الواجبات أصبح الآن عن طريق الحاسوب، حتى التصحيح أحياناً، أو ما يسمونه «كشف الانتحال»، في البحوث وغيرها أيضاً أصبح عن طريق الحاسب، بل بعض الطلاب بدأ يستخدم الذكاء الاصطناعي في حل الواجبات، وهذه سببت إشكاليةً وتحدياً للتعليم.

تقنيات قادت موجة التطوّر الرقمي

قد يكون التطور في عالم التقنية مُزعجاً للمتخصصين وغير المتخصصين بالتأكيد؛ لأننا في تخصصنا يجب أن نواكب هذا التطور، ويجب أن نفهم المواضيع الجديدة، ويجب أن نحاول حتى نسبق هذه المواضيع الجديدة؛ فالتحدي جد كبير، ولا بدّ أنك كل فترة وفترة تتطلع إلى ما هو الجديد من التقنيات؟ وماذا يوجد من أساليب جديدة تقدر أن تستغلها، ففي عصرنا الحاضر تنحصر التقنيات الرئيسية الموجودة الآن في ثلاثة أمور:

1. إنترنت الأشياء.
2. الخدمات السحابية.
3. الذكاء الاصطناعي.

فإذا تكلمنا عن إنترنت الأشياء، فنحنُ نتكلم عن

الأجهزة الصغيرة، والمستشعرات التي أصبحت الآن تستخدم بزخم، وإذا جئنا إلى المؤسسات الحُكومية نجدها مُعتمدةً عليها في كثير من القطاعات مثل هيئة البيئة، وإذا جئنا إلى الشركات الخاصة أيضاً فهي مُعتمدةٌ عليها؛ فشركة إس تي سي (STC) وشركات الاتصالات، أو شركة المياه وغيرها، الكل مُعتمد على هذه المستشعرات، فوظيفتها تجميع البيانات وتجميع «الداتا» أياً كان نوعها، والبيانات عددها ضخم، وكثير من البيانات تقوم هذه المستشعرات بتجميعه، فإلى أين تذهب؟

وهنا سنتكلم عن الخدمة السحابية، من منظورين، من الجزئيتين اللتين تدعمهما أكثر شيء فيها وهي:

- تخزين البيانات.
- معالجة البيانات.

نتكلم عن كميةٍ ضخمةٍ وكبيرةٍ من البيانات، ما الذي سيستوعبها؟ حاسوب شخصي؟ حتى لو قلنا «سيرفر» موجود في شركة، من الصعب أن يستوعب هذه الكمية الضخمة من البيانات، فنحتاج الخدمة السحابية التي عادةً تقدر أن تُقدم لنا مُرونةً في التعامل، وتقديم الخدمة، وتوسّعها، أو تُنقص من إمكانياتها بالشكل، أو بالأهداف التي تراها

الشركة في لحظتها وفي وقتها.

وسنتكلم عن مُعالجة البيانات التي تتم أياً كانت محليةً (Local) أو على الخدمات السحابية؛ فهنا نأتي لنتكلم عن الذكاء الاصطناعي؛ ونُسمي الآن عصرنا، «عصر الذكاء الاصطناعي»؛ لاعتمادنا الكبير عليه، ولا نستثني أحداً في استخدام الذكاء الاصطناعي، فكلّ طبقات المجتمع تقريباً يستخدمون الآن الذكاء الاصطناعي بطريقةٍ أو بأخرى؛ لو نذهب للمحاكم، القُضاة يستخدمون الذكاء الاصطناعي لصياغة -مثلاً- بعض المحاضر عندهم، ولو نذهب لبعض القيادات وبعض المجالات -مثلاً دعنا نقول- الأمور المالية والبنكية قد يستخدمون الذكاء الاصطناعي لمساعدتهم لاتخاذ بعض القرارات، وإذا جئنا إلى الطلاب فقد صاروا يستخدمون الذكاء الاصطناعي في حل الواجبات، فالذكاء الاصطناعي الآن مُسيطرٌ علينا في كل حاجة، فهذه كانت التقنيات الثلاث الأساسية التي أرى أنها هي الآن سمة عصرنا.

فالخلاصة أنّ إنترنت الأشياء **Internet of Things** هي مصدرٌ لعددٍ ضخمٍ من البيانات و بأشكال مُتعددة، والحوسبة السحابية هي من ساعدتنا على تخزين ومُعالجة هذه البيانات، واستخدمنا الذكاء الاصطناعي في المعالجة وفي مساعدتنا على فهم واستخلاص بيانات تُساعدنا في صنع القرار.

عوامل ساهمت في نجاح مُبادرات التحوّل الرقمي

لو نظرنا إلى برنامج التحول الوطني الذي يهدف إلى تطوير البُنية التحتية اللازمة، وتمكين القطاعات العامة، والخاصة، والقطاع غير الربحي، سيلفت نظرنا اثنان من المستهدفات؛ أولاً: تنمية الاقتصاد الرقمي، وثانيًا: الارتقاء بجودة الخدمات المقدمة للمواطنين. وفعلاً، نلحظ الآن أن بعضاً أو كثيراً من الخدمات بدأت تتحول إلى خدمات رقمية، وبالتالي نستطيع أن نرتقي بجودتها؛ فكل شيء عندما يكون مُحكّماً يختلف عما إذا كان يدوياً. أيضاً، الاقتصاد الرقمي، كما نحن نُلاحظ الآن، قامت تجارات بدون مبانٍ، مبنية على تطبيقات، ولعل بعض التطبيقات -مثل «أوبر» وتطبيقات التوصيل، كلها مبنية على تنمية الاقتصاد الرقمي، ما الذي نحتاجه حتى ننجح في قضية التحول وتحقيق المستهدفات؟ نحتاج بُنيةً تحتية، ونحتاج إصلاحات تنظيمية، كذلك نحتاج تشريعات، وهذه كلها سعت المملكة لأن توفرها بشكلٍ أو بآخر، فعلى سبيل المثال لعلنا نذكر مثالاً على مُحاولةٍ في مجال التعليم في التطوير التقني، وكانت في إحدى الدول الآسيوية، كان عندهم حُلم باستخدام التعليم الإلكتروني، وفعلاً بدأوا بإنتاج مواد وفيديوهات.. وكذا، لكن فوجئوا أن

الإنترنت عندهم كان ضعيفاً في ذلك الوقت، وبالتالي يمكننا نقول تأجل المشروع، أو فشل المشروع، وبعدما تطورت شبكة الإنترنت، وأصبح يمكن نقل هذه البيانات (Data)، أصبح بالإمكان فعلاً أن يتم التعليم الإلكتروني عن بعد، وهذه من الأشياء التي من المفروض حينما نُقدم على أي تطوير تقني، أو تحول تقني دراسته من جميع الجوانب، فمن المهم جداً تجميع البيانات الصحيحة؛ لأنك إذا جمعت بيانات، أو معلومات غير صحيحة، ستقودك إلى تخطيطٍ غير صحيح، أو اتخاذ قرار غير صحيح، فلا بدّ أن تكون البيانات صحيحة، ولا تكون فيها أخطاء، أو حتى مُلفّقة، يجب أن تكون دراسةً واقعيةً لواقع الحال وكيف يمكن الانتقال إلى المرحلة التي تليها؛ فوجود التطور التقني، وحماية المعلومات، ووجود الإصلاحات التنظيمية، والبُنية التحتية، هذه كلها مُمكّنات للتطور التقني بإذن الله تعالى.

المحور الثاني

التشريعات المُنظمـــة لحماية البيانات

نرى الآن في الجهات الحكومية والتعليمية تبنٍ للتقنيات الحديثة، مثل الذكاء الاصطناعي، وغيرها من تقنيات البرمجيات كخدمة (SaaS)، **Instruction SAS**، وجميع التقنيات، فيوجد تلهف سريع من الجهات، فكيف يمكن للمؤسسات تحقيق التوازن بين هذا التبني السريع للتقنيات الحديثة وضمان استمرارية هذه المبادرات على المدى الطويل؟ قد تكون بعض التقنيات ما زالت لم تصل إلى مرحلة النضج إلى هذا الحد، ومن باب المسابقة، ومن باب الحصول على هذه التقنية أو تجربتها، تتبناها بعض الجهات في إدارة التحول الرقمي، فتعمل الدولة على قدمٍ وساق في هذا الموضوع، وهم واعون بالبُنية التحتية وأهمية البُنية التحتية، فمن هذا المنطلق بدأت؛ ويوجد كثيرٌ من المشاريع الوطنية التي بدأت، ويُعتبر الإنترنت «حقاً لكل مواطن». ولو ذهبنا إلى كثير من الدول –دعنا نقول الدول المتقدمة– فلن تجد عندهم هذا التعريف بأن «الإنترنت حق لكل مواطن»، بينما هنا في السعودية الآن الإنترنت حق لكل مواطن؛ لأن جميع الخدمات الحكومية الآن تعتبر رقمية. ولا يمكن أن نشرّع شيئاً ونبدأ بشيء إلا إذا تأكدنا من بُنيتنا، والحمد لله الدولة الآن نجحت في ذلك ليس في المدن فقط بل نحن الأن نحال الوصول إلى الأماكن النائية، النائية جداً والمقطوعة وهذا العمل جارٍ فالبُنية التحتية جداً مهمة.

فمن هذا المنطلق، اشتغلت «سدايا» على مشروع وطني، وهي السحابة الوطنية، شبكة او سحابه اسمها «ديم»، هذه السحابة تُعتبر بُنيةً مرنةً تدعم بها جميع القطاعات الحكومية؛ فأيّ قطاعٍ حكوميٍ يُريد أن تكون لديه خدمةٌ سحابية، فقد وفرتها لهم «سدايا» الآن، فتُسرّع من وتيرة التحول الرقمي لأيّ إدارة حكومية، ونحن نعرف الآن أنّ كلّ الإدارات الحكومية ليست مُتساوية وليس تقدمها في التقنية واحد؛ فإذا أتت «سدايا» واستلمت هذا الموضوع –مثلاً– في الحوسبة السحابية، ووفرت لنا هذه الخدمة، فهي الآن داعمةٌ لجميع القطاعات الحكومية لتتطور بشكلٍ سريع؛ فمثلاً إذا جئنا إلى وزارة العدل، وننظر إلى التطور الموجود لديها من ناحية التحول الرقمي، سنجدهم سابقين بكثير، ولو عُدنا إلى طبيعة عملهم وخبراتهم الأساسية، فلا توجد لديهم خلفية تقنية، وأغلبهم خلفية قانونية، وخلفية شرعية، وخلفية إدارية، ولكن مع هذه الممكّنات استطاعوا أن يُطوروا من وضع المؤسسة والوزارة بشكلٍ مَلحُوظ.

ونأتي أيضاً إلى حوكمة البيانات؛ هذه أيضاً من الركائز الاستراتيجية المهمة، فإذا أردت الاستدامة، لا بدّ من حوكمة البيانات، وإذا أتيت لتبني البُنية التحتية، فقد كانوا في نفس الوقت يعملون على حوكمة البيانات؛ فماذا نقصد بمن

هو مالك هذه المعلومة؟ وإذا كان عندنا مجموعة من البيانات مُخزنة في «سيرفر» أو في مكان مُعين، فمن المسؤول عنها؟ ومن المحاسب عليها؟ لا بدّ أن يكون هناك تعريفٌ واضحٌ لها؛ بحيث يُحدد لنا المسؤولية، من هي الجهة المسؤولة عن هذه البيانات؟ وكيف يتم استخدامها بطريقةٍ آمنة، وبطريقةٍ قانونيةٍ آمنة؟ ومن يصدر اللوائح والأنظمة في هذا الموضوع. هنا سنجد عندنا هيئة الأمن السيبراني و«سدايا» يعملون في الأمور التشريعية، وقد أطلقوا كثيراً من اللوائح التشريعية في هذا الموضوع.

تأتي الاستثمارات في الكفاءات الوطنية لتطورنا نحن كطورٍ مجتمعي، يدخل معنا فيه القطاع الخاص والقطاع العام؛ فالآن جهّزت لنا الدولة، وهي تعمل بجدٍ لتهيئ لنا هذا التحول الرقمي، ولكن كيف يمكننا نحن أن نشغل هذا التحول الوطني وهذه الأنظمة الرقمية من دون كفاءات؟ حتى لو «خرّجنا دفعةً واحدةً متمكنةً»، فهذا لا يكفي، ونحن لا بدّ أن نعمل على تطوير الكفاءات التي تواكب هذا التطور بالتقنية؛ بحيث إذا توفرت عندنا هذه التقنية، وعندنا كفاءات وطنية –مثلاً– في كوادر الأمن السيبراني أو في الأمور الهندسية، تقدر أن تدير هذه الأنظمة، وتطور هذه الأنظمة، وتغلق ثغراتها إذا وُجدت. فهذه ثلاث ركائز

أساسية؛ نتحدث نحن عن:

- الحوكمة.
- البنية التحتية.
- الاستثمار في الكفاءات الوطنية.

وكلها لا بدّ أن تتوفر، وإذا توفرت، بإذن الله، فإنّ أيّ تطورٍ سيكون -إن شاء الله- مُستداماً، وستكون وتيرته سريعة. وتجربة المملكة في التطور التقني وتقديم الخدمات تجربةٌ تُدَرّس، حتى في بعض -أو نقول أغلب الدول الغربية- فحينما نسافر إلى أمريكا أو أوروبا، لا نجد مثل الخدمات الموجودة في «أبشر»، والخدمات الموجودة في «توكلنا» وكان أفضل مثالٍ لما جاءت جائحة كورونا وكان عند الأشخاص في الجوال في «توكلنا» الحالة الصحية، وكانوا يعرضونها في المطار، فكانت تجربةً تُدَرّس في جميع الجهات.

المحور الثالث

التحديات الأمنيـــة

نحن حقاً في تطور، وكثيرٌ من الناس يجهلون ذلك؛ لأنهم يعيشون في البلد وفي هذه النعمة، ولكن الذي يذهب ويُسافر ويعيش خارجاً يشاهد كيف التطور الموجود عندهم، كيف هم مُتأخرون في موضوعٍ كهذا، ونحن متقدمون بكثيرٍ في نظام التطور الرقمي، والمشكلة التي من الممكن أن تبرز من خلالها هي أنك وفرت كميةً كبيرةً من البيانات في مواقع رئيسية، وهذا سوف يكون تحدياً علينا نحن أهل البلد، كيف نحميها؟ لأنها الآن كما يقولون تعتبر منجم ذهبٍ لكثيرٍ من قراصنة الإنترنت، فلا بدّ من حمايته.

ولا ننسى دائماً أن أي تطورٍ تراه له سلبياته وله إيجابياته؛ فالتطور الذي نحنُ نستخدمه، يوجد غيرنا يستخدمونه بطريقة سلبية، فمع الذكاء الاصطناعي تولدت لنا طرق جديدة وحديثة في الهجمات، فعندنا الآن تزايد في الهجمات، إذا تكلمنا عن الهجمات السلوكية التي هي **Social Engineering** (الهندسة الاجتماعية)، وعندنا هجمات الذكاء الاصطناعي التوليدي للتصيد الاحتيالي أو الهندسة الاجتماعية **Generative AI Attacks for Phishing or Social Engineering**، وعندنا أيضاً في الذكاء الاصطناعي الذي يستخدمونه في الهجمات «**Agentic AI for Automated Attack**» فأنت الآن

توظف الذكاء الاصطناعي وهو الذي يعمل لك **Attack** (الهجوم)، ويُغير من أسلوبه، ومن طريقته، ومن عمله بحيث يستطيع أن يخترق الموجود أمامه، أو يُعيد دراسة الشخص الذي أمامه والذي يريد أن يُهاجمه؛ بحيث أنه يقتبس من الإنترنت ما هي المعلومات المتوفرة له، ويُحبك القصة عليه، فهذه كلها أمور خطيرة ما جاءتنا إلا مع التطور، نحنُ نريد أن نتطور، ولكن في نفس الوقت نريد أن نحمي أنفسنا.

ونأتي إلى المؤسسات الناشئة، والمتوسطة، والصغيرة، سنجد إشكالية، فعادةً الموارد التي عند هذه المؤسسات خاصةً الناشئة والصغيرة دائماً مُحدودة، فليس عندهم القدرة لتوظيف شخصٍ مُتخصصٍ في الأمن السيبراني ولا توفير الأجهزة، أو الدفع للمؤسسات ليغطوا لهم هذا المجال؛ فهنا دائماً مشكلة، فلا بدّ أن يُوجد برنامجٌ وطنيٌ لدعم هذه الفئات لتطويرها؛ لأنه إذا كنت تريد أن تبحث عن ثغرةٍ في نظام، فدائماً ستجدها في الحلقة الأضعف، وهؤلاء هم الحلقة الأضعف فدائماً المدخل منهم، وإذا أردنا أن نُوسع الدائرة أكثر وأكثر، فأكبر حلقة موجودة هي الثغرة البشرية، أينما كان، حتى مع العمل الكبير الذي فعلته الدولة والعمل في الأنظمة والتشريعات، يظل الموظف الموجود في قطاع حكومي، حتى لو وضعوا عليه ألف نظام أمني، يظل هو الحلقة الأضعف، فقد يكون بسبب جهلٍ منه، أنه أعطى

كلمة مروره لشخصٍ ما وهذه ترونها كثيراً في القطاعات، فيبقى علينا نحنُ كمتخصصين في الأمن السيبراني التوعية، وإذا وجد قطاع في إدارة حكومية، فيوجد فيها إدارة خاصة للأمن السيبراني، وظيفتها التثقيف للموظفين، وأساساً هذا من ضمن الأجندة، من ضمن الحوكمة الموجودة، أنه لا بدّ أن يركزوا على الموظفين ويثقفوهم، وإذا كنا نحنُ نتكلم عن الثغرة البشرية من ناحيتنا كمجتمع، كأفراد، فيقع علينا نحنُ كتقنيين أن نثقف المجتمع، وإخواننا، وأهلنا، وأصدقاءنا بالمخاطر، وبالشيء المفترض أن يفعلوه، فهذه مشاكل تحدث بكثرة، وهذه عادةً الثغرة التي دائماً تحدث في المؤسسات الصغيرة، وهذه مشكلة دائمة وأزلية موجودة عندنا من قديم.

تكامل التشريعات الوطنية مع المعايير الدولية لحماية البيانات

إنّ البيانات هي ثروةٌ وطنيةٌ، مثلًا لو جاءك شخص وقال لك أنا والله أريد أن آخذ البترول الموجود في المملكة العربية السعودية، وأستغل ذلك، تجد الناس تقوم لهم قائمة ولا يقعدون، ولكن في موضوع البيانات قد لا يكون لدى الأشخاص هذا الإحساس فعلياً في داخلهم، وإنّ الأنظمة عندنا، أو نظام حماية البيانات، أو نظام التعاملات الإلكترونية وغيرها لا تأتي من الصفر، وإنما دائماً يُستند

فيها للعرف العالمي وما يتماشى معه ، حتى لا تكون خارج النطاق؛ فنظام حماية البيانات بلا شك يتماشى مع حماية البيانات الشخصية، بمعنى أنا بياناتي موجودة عند الجامعة كطالب، ويُفترض أنها لا تخرج بدون إذني، وهناك جزءٌ من البيانات يُسمح بخروجه لجهات مُعينة، أما الباقي فهي بياناته الشخصية، وكذلك النظام يُنظم، أو يُرتب كيف يتم التخلص من هذه البيانات أو إخفائها، ووجود البيانات بشكل رقمي دائماً يُعتبر خطراً ومُهدداً، وإذا لم يُوفر لها الحماية الكافية، ربما يحصل اختراق أو شيء خطير، ودائماً نسمع أن بعض الشركات تم اختراق قاعدة البيانات عندهم وسرقة البيانات، فوجود هذه التشريعات والأنظمة بما يتسق مع الأنظمة العالمية بلا شك أمرٌ ضروريٌ ومُهم، وهذا هو المِمارَس ولله الحمد عندنا في المملكة.

يبقى الآن الدور علينا أيضاً كأفراد؛ الشخص يجب أن يكون واعياً، وهذه يمكن ملاحظتها أيضاً في الحملة التي يقوم بها البنك المركزي مع البنوك والتي تقول: «خليك نبيه»، فهي نوع من التوعية للاحتيال المالي الذي هو شكل من أشكال الهندسة الاجتماعية **Social Engineering**، وهذه التوعية بلا شك ضرورية؛ وذلك لتجدد أساليب الطرف الآخر، فكلما تجدد أسلوب المجرمين، لابد أيضاً رجل الأمن أن يكون

نبيهاً ويستطيع أنه يُعالجها، لكن هذا لا يعفي الشخص أن يُحافظ على ما لديه. تقول له: يا أخي أغلق بابك! حافظ على بياناتك! فيقول: أنا لا يوجد عندي شيءٌ أخاف عليه في جهازي، ويقول: أتركهم يأخذون، أتركهم يدخلون. إنّ الخطر ليس فقط أن يأخذوا من جهازك، الخطر الحقيقي أنهم يستخدمون جهازك كمنصة للانطلاق إلى مكان آخر أو أنهم يسرقون بعض البيانات التي عندك للدخول على أنظمة أخرى. فبلا شك أن التوعية ضروريةٌ ومُهمة، وهي تتماشى مع باقي المقومات التي تدعم التحول الرقمي.

الذكاء الاصطناعي في حماية البيانات

كان فيما سبق في الهندسة الاجتماعية يكفي أنه يعرف اسمك ومنصبك وكذا ثم يذهب يتصل على مسؤول النظام **System Admin** ويقول لها أنا الدكتور فلان وأريدك أن تفعلي لي إعادة تعيين كلمة المرور **Reset** لـ **Password** وكذا، أما الآن فتطورت التقنيات فالذكاء الاصطناعي الـ **AI** يمكنه أن يدخل في الموضوع، ونشاهد كثيراً من التزييف العميق الـ **Deep Fake** الموجود، تقوّلٌ على بعض الناس، أفلام فيديو وغيرها، فبلا شك مع تطور الـ **AI** وإمكانية استخدام ما يسمونه الذكاء الاصطناعي التوليدي، وأيضاً

هناك تطور في خط موازٍ له، وهو ما نسميه الذكاء الاصطناعي الأمني، بمعنى توظيف الذكاء الاصطناعي في المجال الأمني في مُحاربة الهجمات والمخاطر بذكاء إصطناعي، وهذه موجودة والعمل فيها قائم فهي دائماً كما نقول على طرفين، هذا يتقدم وهذا يلحق به في مُحاولة للمُوازنة، ويبقى الشخص هو المحور الأساس والحلقة الأضعف التي يجب أن نركز عليها ونهتم بتوعيتها، يقال أن ٧٠٪ من الاختراقات سببها شخص داخل المنظومة، وليس من خارجها. الجهات تبذل ما لديها في حماية أنظمتها، ولكن يأتي القصور بعض الأحيان من الداخل.

إنّ استخدام الذكاء الاصطناعي في حماية وأمن المعلومات هو ضرورة لكنها تعتمد على المستوى الذي وصل له الذكاء الاصطناعي في الحماية، فإذا وصل إلى مستوى يمكن أن يوثق به، فبلا شك أنه قد يصل إلى أنه ضرورة أو يجب أن يُستخدم، لكنه إذا كان مشكوكاً في فعاليته، فبلا شك قد يتخوف الإنسان من استخدامه، ومع التطور الموجود الآن في الذكاء الاصطناعي، قد يأتي نوعٌ من الانتكاسة، وقد بدأت ظواهرها تبدأ، حيث الناس بدأوا يشككون في كل ما حولهم؛ فعندما يصلك مقطع فيديو أو مقطع صوت، أو حتى أنت كأستاذ في الجامعة ويأتيك واجب، أو حتى

كمدرس ابتدائي ويأتيك طالب حل الواجب، تبدأ تشك هل هو الذي عمل هذا، أو أن هذا مُولّد عن طريق الذكاء الاصطناعي؟ فربما تحمل الأيام القادمة مفاجآت، وما ندري ما الذي سيكون.

وليس هذا أول تطورٍ يشهده البشر، فقد جاءت الثورة الصناعية وذكر الناس كيف سيتأثر دور البشر في هذه الثورة، والإنسان من ميزته دائماً أن يتكيف مع الوضع ومع الحالات؛ فإذا دخلنا على عصر الأتمتة، يظل البشر موجوداً، ولكن دوره سوف يتطور، فبدل أن يكون هو العامل، وقد أزيلت وظيفته كعامل، ولكننا نحتاجه الآن في دور آخر، فالآن نريده أن يكون في مهام استراتيجية، وتحليلية، ورقابية، نحتاج شخصاً يقوم باختراع هذه التقنية، نحتاج شخصاً مُبدعاً ومُبتكراً، ونحتاج شخصاً يُشرف على هذه الأداة، ونحتاج شخصاً يديرها، ونحتاج شخصاً يبيعها، ونحتاج شخصاً يقوم بصيانتها؛ فحتى لو جاءنا عصر الأتمتة ودخلنا عليه، ونحنُ أساساً على مشارفه، ورتم التطور الآن فيه سريع، فأنا كبشر لازم أتغير وأتكيف، أما إذا جلست تقول: لا أنا ما أقبل، لا أتطور، فأكيد سوف تخسر، ولكن لا بدّ أن تؤمن وتتكيف وتتطور معه.

المهارات التخصصية للتكيف مع التطور التقني

لو أنّ شخصاً تخرّج من الحاسب بتخصص ذكاء صناعي، ويتوقع أنه الآن حصل على أحدث نوع من التقنية، فيظن أنه مُتمكن في كل شيء، فهذا خطأ، صحيح أنَّ من أكثر الأعمال والوظائف الموجودة هنا الذكاء الاصطناعي، وممكن حتى يكون الأمن السيبراني ، لكن هناك تخصصات ثانية مهمة في تحليل البيانات **Data Analysis**، ولكن لا بد أن يتكيف كما قلنا، ويتطور، فإذا كنت مثلاً تحب تخصص نظام الأمن السيبراني لا بدّ أن تدخل أعمق ما فيه، فتهتم بالأمن السيبراني السلوكي، ولا بدّ أن تطور نفسك وتصبح مُتميزاً في هذا المجال، وتفهم دوافع المهاجمين وأنماط الهجمات، وتتابع تقنيات حديثة من الممكن أن تستغلها من أجل أن تكون مخترق أبيض (وايت هاكر) وتستطيع أن تتصدى للمهاجمين في المستقبل. وحري بك معرفة بعض التخصصات الثانية، **Interdisciplinarity** ، فلا تغلق نفسك على تخصصك فقط، وتقول أنا في مجال التقنية فقط، ففي الأخير ستمضي سنوات بسيطة من حياتك فيها، وبعدها أساساً ستتطور، وربما تكون مدير إدارة، فيتحتم عليك أن تتكيف وتتعلم تخصصات ثانية، ومجالات أخرى، فلو أتينا بمهندس أمن سيبراني ووظفناه في

دائرة الأمن السيبراني في بنك، لن يفهم المعاملات البنكية ونظام المدفوعات، ولن يفهم كيف يُطوّر لهم نظاماً حتى يدرس النظام المالي ويلم به ، حيث يوجد ترابط **Interde-pendence** ، من ثم يقدر يبدع فيه ويكيف نظام أمني عليه. وطبعاً نحنُ كأكاديميين مُقصرين كثيراً في حوكمة البيانات، ما نضمنه في مقرراتنا، لن أتكلم عن البرامج، في بعض البرامج يضيف مقرر أو مقررين، ولكن أنا لا أرى أنه لازم نضيف مزيد من المعلومات، حتى لو بشكل غير مُباشر للطلاب في حوكمة البيانات في ظل اللوائح والقوانين السعودية، لأنَّ الطالب إذا نزل السوق هو أساساً يتوقع أنه قادر على استخدام البرنامج كما هو، لا. يوجد أنظمة، يوجد قوانين الآن تحكم في البلد، فلابد نحنُ نعرضهم لها، لا بد ندخلها لهم بشكل مباشر.

هنا نأتي كأعضاء هيئة تدريس، كمُعلمين، وتأتي أيضًا «سدايا»، وهيئة الأمن السيبراني، لا بد أن يكون بيننا وبينهم تواصل؛ بحيث أنهم يقدمون لنا اللوائح بشكل يسير، ونحنُ نبحث عنها بحيث نقدمها للطلاب، لأن هذه أراها عقبة كبيرة أمام الخريجين الشباب الناشئ إذا نزل إلى سوق العمل، فإذا كان فاهم، وإذا تطور من نفسه فيها يستطيع يختصر عمل كثير.

لا تفصلوا الأمن عن الابتكار، ولا يكون تخويفنا من الأمن مانعاً للابتكار، أن أيّ تطور نحتاجه يبدأ من إدارات واعية، ومن هذه الإدارات الواعية ندرك أن الأمن لن يكون حاجزاً أمامنا، إنّ الدور الذي يلعبه العنصر البشري في ظل الأتمتة والتحول الرقمي كبير، ولو فكرنا في العنصر البشري سنقسمهم قسمين: مُستخدم، ومُطور؛ فالمستخدمون يتفاوتون، بعضهم نسميه، المبتدئ، وبعضهم المحترف، والمتمكن من الأداء وخاصة الجيل الحديث، لكن في النهاية هم يظلون يحتاجون نوعاً من التوعية، ويحتاجون نوعاً من التدريب، ويحتاجون أن يكون تصميم هذه التطبيقات مُتماشياً مع قدراتهم، وسهل الاستخدام، ويُقلل الأخطاء البشرية. أمَّا من حيث المطورون وهم المبرمجون، فبلا شك أنَّ المسألة ليست مسألة كتابة برنامج، لكن يجب أن تنظر لعدة مناظير؛ منها المنظور الأمني، أنَّ البرنامج يكون آمناً غير قابل للاختراق قدر الإمكان، وأن يكون سهل الاستخدام، أيضاً حتى يتمكن المستخدمون من الوصول لما يهدفون له بسهولة، وهذه أتصور من أهم الأدوار للعنصر البشري بنوعيه في مجال التحول الرقمي أو التطوير الرقمي.

مهارات سوق العمل

في السابق كان المهارات المطلوبة هي: الذي عنده مهارة الطباعة باللمس، وتنظيم الوقت، ومهارات كتابة العروض، أو الكتابة عموماً، هذه كلها كانت مهارات مطلوبة، ولا زالت مطلوبة، لكن الآن دخلت علينا مهارات جديدة؛ كاستخدام الذكاء الاصطناعي؛ حيث يختصر عليك الوقت في بعض الأشياء، وممكن استخدامه أيضاً في البرمجة وإن كان هذا قد يُعتمد عليه اعتماداً كلياً في ذلك، وأيضاً مهارات استخدام التقنيات الحديثة في المختبرات وفي تحليل الدم وغيرها، الآن أصبح هناك جهاز تضع فيه العينة، ثم خلال وقتٍ وجيزٍ يقوم بعمل عدد من التحاليل، لم يعد مثل السابق، في كل تحليل يحتاج له مهارة مُعينة، والأشعة نفس الشيء، بل حتى يمكن استخدام الذكاء الاصطناعي في الأشعة، وتحليل الصورة، وكتابة التقرير الذي يقرأه الطبيب، فالمهارات ستتغير تبعاً لتطور التقنيات، لكن المهارات الأساسية تبقى هي الأساس، ولا يمكن أن ينفك عنها أيّ شخصٍ سواءٌ كان مُتخصصاً في التقنية، أو حتى في سوق العمل.

إنَّ أمن المعلومات يجب أن يكون متطلباً في جميع التخصصات باختلاف أطيافه بحسب التخصص، وهو دخل في بعض الأشياء. الذكاء الصناعي بلا شك أنَّه أداة قوية

ومفيدة وقد تكون ضارة، فدخوله في التخصصات سيكون مفيداً إذا دخل بشكل صحيح، بمعنى ألا يكون هناك اندفاع وراء هذه التقنية، واسترسال بدون تحديد تبعاتها. والتطور الرقمي هو التغيير، لأنك تتغير من شيء إلى شيء، من طور إلى طور، من تقنية إلى تقنية، أو من حال إلى حال، فبعد استخدام الورق، بدأنا نستغني عن الورق، وبدأنا نستخدم الذكاء الصناعي، فهي عملية تغيير، وليكن التغيير مدروساً وليس تغييراً اندفاعياً، وإنما يكون مدرُوساً بمعنى يحسب حساب التنظيمات اللازمة، والتقنيات اللازمة، والأمن من جميع العوامل، حتى لا يكون هذا التغيير غير فعَّال أو غير ناجح.

مداخلة معالي الدكتور/ عبدالقادر الفنتوخ

عضو هيئة التدريس بجامعة الملك سعود و وكيل وزارة التعليم العالي للتخطيط والمعلومات سابقاً

وهناك تذمرٌ من بعض أساتذة الجامعات من استخدام الطلاب الذكاء الاصطناعي في حل الواجبات، ورأينا بعض المقاطع في ذلك، ليس في العالم الثالث، بل حتى في أمريكا متذمرين جداً ويضرب على الطاولة ويشتكي ويسب ويذكر ألفاظاً غير مقبولة إلى آخره، والمشكلة ليست من الطلاب ولا هي من الذكاء الاصطناعي، وإنما المشكلة من الأساتذة

الذين هم بعيدون كل البعد في فهم علاقة الذكاء الاصطناعي بالعملية التعليمية، كان بإمكان الأساتذة عندما يجهز واجباً وهو يعرف أنَّ الطلبة سيستعينون بالذكاء الاصطناعي وجوجل وغيرها، أن يضع أسئلةً يتحدى بها الطالب ويحفزه على التفكير وإيجاد الحلول، وأيضاً يحفز الذكاء الاصطناعي بإجباره على إيجاد نتائج مُفيدة وجميلة لكل طالب على حدة، مثلما كنا نأخذ اختبارات الكتاب المفتوح، فكان الأساتذة يعرفون كيف يصيغون الأسئلة في هذا الخصوص.

منذ ٦٠ سنة تقريباً جوردن مور انتقل من شركة **chips** وغيرها إلى شركة **Intel** أو أسس **Intel** مع شخصين آخرين، ورأى أنَّ عدد الترانزستورات في الرقاقة الواحدة ممكن تتضاعف كل سنتين، والواقع اليوم يشهد تضاعفاً خيالياً؛ فمثلا في عام ٢٠٠٠ عدد الترانزستورات في الجوال المتقدم الموجود في الشاشة والذاكرة والبطارية إلى آخره يمكن حدود 15 مليون ترانزستور، بينما في الجوالات اليوم – الجولات المتقدمة – عدد الترانزستورات ٢٠ مليار ترانزستور، فيوجد قفزة كبيرة جداً ساهمت في زيادة السرعة، سرعة المعالجة، واستهلاك أقل للطاقة، وكفاءة أعلى، وتفاعل مع الذكاء الاصطناعي، وذاكرةٌ عاليةٌ، وشاشاتٌ واضحةٌ إلى آخره.

إنّ الشعار الذي رُفع في المملكة العربية السعودية وهو «الإنترنت حق لكل مواطن»، لا بدّ أن يكون لأغراض التعلم المستمر، ولأغراض التواصل مع الحكومة، ولأغراض الاستفادة من الخدمات، وطبقاً لتقرير منظمة«**We Are Social**» في عام (٢٠٢٥)، فإنَّ نسبة انتشار الإنترنت في المملكة واستخدام منصات التواصل الاجتماعي يشكّل ٩٩٪ من إجمالي السكان سعوديين وغير سعوديين إلى آخره، وهذه تُعدُّ من أكبر النسب على مستوى العالم، طبعاً أكيد الترفيه والخدمات جعلنا جزءاً من الفضاء السيبراني، فهذا يؤثر علينا ونحاول أن نؤثر فيه، وطبعاً الفضاء السيبراني مليء بالمعلومات والخدمات، إلا أنه أيضاً مع الأسف مليء بالمخاطر التي من الممكن أن تؤثر على بياناتنا وخصوصيتنا وأجهزتنا.

مخاطر التقنية

إنّ حماية مؤسسةٍ ما عملية صعبةٌ جداً، فلا بدّ أن تحمي المنشأة نفسها بمبانيها وأفرعها، ولا بدّ أن تحمي الأفراد عندما تُجري مقابلاتٍ شخصيةً معهم وتوظفهم، وأيضاً دخولهم، وخروجهم، وكروتهم، وأيضاً الموظفين والعاملين والزوار، وسلاسل التموين، والخدمات، وأيضاً الأمن التشغيلي الذي هو تأمين الشبكات، والأجهزة، واللابتوبات، والجوالات

إلى آخره، وأيضاً البيانات، والتطبيقات والحوسبة السحابية إذا كانت الجهة عندها حوسبة سحابية وطريقة للعمل عن بعد، وأيضاً أمن حسابات البريد، وشبكات التواصل الاجتماعي من المهم المحافظة عليها، وتسجيل الرُخص أن تسجل بطريقةٍ آمنةٍ من حيث الملكية الفكرية، ومن حيث ضبطها أمنياً لكي لا تأتي بتبعات سلبية. والأفراد الذين يعملون في المؤسسات الحكومية والخاصة يواجهون أخطاراً كثيرة، من أبرزها؛ انتهاك الخصوصية، وانكشاف معلوماتنا الخاصة والسرية، ويتسبب في بُطْئ الأجهزة، وتعطل الخدمة أحياناً، ورسائل التصيد، والابتزاز، وبرمجيات انتزاع الفدية الـ **ransomware**، أيضاً التعدين القسري الذين يستغلون جهازك؛ بعض الناس يقول: «اتركه يا أخي يرى جهازي ما فيه شيء أصلاً». لا، جهازك فيه كهرباء، وفيه موارد، ويكون بطيئاً، لأنَّ بعض الناس ممكن ينزل عندك برامج تعمل تشفير **crypto**، وما يسمى العملات المشفرة بـ **crypto jacking** الـ **crypto mining**، وهو التعدين للعملات، يمكن يعدن عن طريقك ويستفيد من الـ **GPU** والـ **CPU** الموجود عندك وإلى آخره، ومعظم البرامج الخبيثة هي موجودة في معظم البرامج المكسورة، في برامج الـ **VPN** التي ينزلونها الناس، في برامج التورنت **tor-rent** وما شابهها من برامج مجانية يبدو أنها بريئة، ولكن وراءها ما ورائها، مثل تنزيل مقطع أو صوت من محاضرة أو

مقطوعةً أو شيئاً من يوتيوب، ففي الغالب ثمانين أو تسعين بالمائة من هذه البرامج تضع عندك تعدين قسري إلى آخره، وأنت تستطيع تفحص ذلك عبر البرامج التي تكتشف أموراً كهذه، وهناك اكتشافاتٌ سريعةٌ تستطيع أن تفعلها؛ فإذا كان جهازك دائماً حار، وإذا المروحة تشتغل وما تنطفئ، وإذا البطارية تفرغ بسرعة، ففي الغالب أنّه يوجد أحدٌ يستفيد من جهازك، أو ينقل بعض البيانات منه.

حلولٌ تقنية

وهناك حلولٌ كثيرةٌ وبسيطة في الحماية، كتأمين شبكة الواي فاي التي في البيت والموجودة في العمل، ووضع كلمات سرٍ ليست افتراضية كالتي موجودة في الـ **access point**، وإخفاء شبكة الـ **Wi-Fi** إن أمكن فهو أفضل بكثير، سواءٌ في العمل أو في البيت، أو الشخصيَّةً، وبعض الناس إذا أرادَ أن يفتح حسابات في الـ **E-mail** وغيرها، يضع حسابات وهميَّةً! لا، ضَعْ معلوماتٍ دقيقةً كي تسترجع حساباتك، وفي الأماكن العامةِ الأفضل عندما تذهب إلى مقهى أو غيره، لا تدخل على الـ **Wi-Fi** الخاصِّ بهم، من الأفضل الدخول على نقطة اتصال في جوالِكَ، هذا آمن لك بكثير، وتحديثُ أنظمة التشغيلِ في الـ **Laptop** والجوالات لا بدَّ أن يتمَّ بشكلٍ تلقائي مُتكرر، وبعض الأجهزةِ يجب

أن تذهبَ أنتَ لتُحدِّثها، ولا نركب برامج مكسورة، أو مجهولة المصدر، ولا بدَّ أن نقومَ بمسحٍ للتطبيقات فأيّ تطبيقٍ لا نحتاجه بشكلٍ يومي أو أسبوعي، نمسحُهُ من الـ **Lap-top**، ومن الجوالِ، وإذا احتجناه بعد أسابيع أو أشهر، ننزله مرة ثانية، فإنَّنا سنجد نسخةً أحدث جديدة، وتسجيلُ الدخول ليس مشكلةً، بل سيوفر لنا متاعب كثيرة، والجوال يجب ألاَّ نكشفهُ فبعض الناس يذهب مباشرةً ليعرّض جوالَهُ للاختراق بـ الـ **Jailbreak** للذين يستخدمون **iPhone**، والـ **root** في الذين يستخدمون **Android** وهذا يعرض جهازَكَ للخطر، وإذا كنتَ تحبُّ المغامراتِ، وتحبُّ اللعب في بعض البرامج، اجعلْ لك جوالاً مستقلاً للتجارب، واجعلْ عليه **Jailbreak** أو **root**، واستخدامُ التحقق الثنائي مهم، أيضاً من المهم أننا في بيوتنا، أو في مؤسساتنا، لا بدَّ أن نضع برنامجاً تدريبياً، إما إلزامياً، أو توعوياً حول مهارات الأمن السيبراني لكي نُعزِّزُ الوقاية، وآلية التعامل مع الاعتداءاتِ.

أهمية العامل البشري

العامل البشري مهم في عملية الحماية؛ حيث أشار تقرير لعدَّة شركات مشهورة، كـ **Verizon** و **Kroll** إلى أنّ السبب الرئيس لانتهاك الخصوصيةِ هو العنصر البشري وبنسبة ٨٦٪ في المؤسسات والقطاع الخاص؛ فإذا لم يُبنى

الوعي للعنصر البشري ويُعرّف بالمخاطر فسيقع في المحظور وأحد فوائد الـ **AI** أنه يقومُ بما يسمى بـ **Auto Enforcement Policy**، فيكتشف الأخطاء البشريةَ ويمنعها من الحدوثِ، ولم نرَ بعدُ أنظمةً قويةً في هذا الشيءِ، لكنَّها إن شاء الله آتيةٌ. والذكاء الاصطناعي أحدث، وسيُحدث أيضاً تغييراً كبيراً في عالم الأمن السيبراني في الدفاع وفي الهجومِ. حتَّى المعتدين والمتطفلين الآن يستخدمون الذكاء الاصطناعي لاكتشاف الثغرات، ويذهبون إلى ما يسمى بـ **Zero Day**، التي هي الثغرات المكتشفةُ ولم يُصدَرْ لها ترقيات، وبرامج الأمن السيبراني الآن المدعومة بالذكاء الاصطناعي كشفت فيروساً اِسمُهُ **Ocean Lotus**، لا يمكن لأيّ برنامجٍ مضادٍ للفيروسات أو بحثٍ شخصيٍّ أن يَجِدَهُ، لكن الذكاء الاصطناعي اكتشف **Ocean Lotus**؛ لأنَّهُ مزروع داخل الـ **Code** الكود، وأيضاً، الذكاء الاصطناعي سواءٌ للدفاع أو الهجوم، يستطيعُ أن يتعرف فورياً على سلوك المستخدمين ويعرف كيف يُسقِطُهُم في مطب، أو كيف يمنعهم من الوقوع في مطبّ ، من الجميل أن نستعينَ بالذكاء الاصطناعي لتوليد الـ **Codes** (الأكواد) وتعديل الـ **Codes** واختبار الـ **Codes**، لكن لا بدَّ للمبرمجِ الذي يفهمُ أنه لا بدَّ أن يعرف (المنصة) الـ **Platform** ويعرف لغات البرمجةِ التي يستخدمها، ولا بدَّ أن يعرف كيف يصمم

خوارزمياتِهِ ويستعينُ بها، ولو ظن أنه فقط يقولُ: «برَمِجْ لي، وأعطني، وضَعْ لي» وهو لا يفهم، فإنَّهُ سيقعُ في مطبات كثيرة؛ لأن الذكاء الاصطناعي ما زال ضعيفاً، لكنَّهُ سيتقوى خلال الفترة القادمةِ — والله أعلم — ومن المحتمَلُ إمكانية أن يبرمج حسب مرئياتٍ مُعينة، ونعتقد أن الزمن تعدَّى مرحلة الـ **Codes** (الأكواد) وما شابهها، فالآن التوجُّهُ إلى ما يسمى **No Code/ Low Code Or Low Code/ No Code**، أنظمة جديدة ومنصات جديدة، ولا يحتاج أنْ تبرمَج على الإطلاقِ، فقط مجرد أن تسحب نوافذ منبثقة وتأخذ بـ الـ **Mouse** ((الفأرة) وترمي هنا وتضع هنا، مثل نظام مثل **Out Systems** وغيره، فلا تحتاج الأكوادِ مُطلقاً، لا شخصيًّاً ولا عن طريق الذكاء الاصطناعي.

ويجب أن يكون البعد الاجتماعي حاضراً في الـ **So-cial Engineering** (الهندسة الاجتماعية)، لكن تبقى قضية الهوية الرقمية والتهديد القيميّ للجانب الرقمي وجانب الذكاء الاصطناعي، وهو ما يحتاج إلى تسليط الضوء عليه من أبعادٍ مُتعدِّدةٍ، وسنركِّزُ على قضية أن الشباب اليوم، بكَافَّةِ أجناسهم؛ ذكورًا، وإناثا بحاجة إلى أن يتعاملوا مع الذكاء الاصطناعي لا على أنَّهُ مصدرٌ موثوقٌ بالجانب القيمِيّ، وجانب الفتوى، وجانب تلقي المعلوماتِ، وهو في تطورٍ

سريعٍ جداً، لكن في الوقت نفسه لا بدَّ أن نوطِّن ونعوِّد شبابنا وأبناءنا وطلابنا على أن يعودوا إلى الكتب؛ ليس لأنه الحنينَ للكتاب وراحة الكتابِ، ولكن لأنَّهُ المصدر الذي يجب أن يكون فِعلاً بين أيديهم. والأمر الأهم من ذلك هو أنّ هذا الفضاء المفتوح الذي كان بين أيدينا مُمَثَّلاً في الجوال أو الهاتف الكفِّيّ أو الأجهزةِ الكفية، أصبح متطوراً الآن، كأنه أصبح ذكاءً اصطناعيّاً، عالم كبيرٌ جداً من البيانات والمعلوماتِ التي إذا دخل الإنسان عليها وهو غير مسلَّح بأدوات السباحةِ، سوف يغرق في هذا التيار الجارفِ؛ فنحتاج فِعلاً إلى الوعي، والوعي يجب أن يكون فِعلاً من نعومة أظفارِ أبنائنا، وهم صغار، من المرحلة الابتدائيةِ، يتعاملون مع الرقميَّاتِ سواءٌ بالألعابِ، سواءٌ عن طريق جوالاتهم أو عن طريق المنصات المختلفةِ، فقد يُستغَلُّونَ ويكونونَ هم ثغرات أمنيَّةً على أجهزتنا وعلى مجتمعنا وعلى قِيَمِنا ومبادئنا. ربما بعد خمس سنوات تقريباً سوف تختفي الأجهزةُ الكفِّيَّةُ ويختفي الـ **Internet**! فما المتوقَّع بعد ذلك من الإخوةِ المختصينَ في جانب الحاسب وجانب الذكاء الاصطناعي؟ وهل فِعلاً هناك تطمينات لهذا التهديد، وهناك أيضاً نوع من التخويفِ؟ هذا التخويف له مبرراتُهُ والتطمين له مبرراتُهُ، لكن كيف يمكن المزاوَجَةُ بينهما، أو الدمج بين الثقة في الدخول في هذا العالم فِعلاً، فالـ **Deep Fake**، فِعلاً غريبٌ جداً أن يكون هناك حصانة من التأثُّرِ

القيميِّ والتأثُّرِ بالمبادئ وتأثُّر المرجعية، وأيضاً مرجعية الفتوى والمرجعية الثقافية الدينية.

ماذا بعد الأجهزة الكفِّيَّةِ؟

يسأل البعض: ماذا بعد الأجهزة الكفِّيَّةِ؟ الله أعلم. سابقاً، في بعض الأفلامِ، يأتون بالشخص يتكلم في يده وهذا خيالٌ علميٌ أصبح حقيقةً واقعةً، فكلّ شيءٍ أصبح مُمكِناً، وسابقاً كان المتخصصونَ في الـ **Satellite** (الساتلايت) وفي الهندسة الكهربائيةِ، يقولون: مستحيل! أن يكون الـ **Dish** (الدش) دِشّاً صغيراً وهكذا، مستحيل بالتقنيةِ الموجودة حالياً! ولكن تغيرت التقنية بعد ما كانت **Analog** صارت **Digital**، وبالتالي استطاعوا أن يصغروا حجم الـ **Dish** فأصبح حجمه صغيراً، فدائماً يكون هناك شيءٌ في المستقبل، ويظهر بعد أن تنجح تجاربه أو بعد أن تنجح أعماله؛ فكلّ شيءٍ ممكن؛ وقد رأينا التجارب أو على اطلاع بالـ **Electron-ic Tattoos** وعلى التجارب التي أقام فيها **Elon Musk** زرع **Chips** الخاصة في الأشخاصِ، وهي لازالت في طور الاختباراتِ والتجاربِ، وربما دخلت في مرحلة الاعتماد لـ **FDA** الأمريكي. فهل نتوقع شيئاً قريباً من هذا النوع؟ ما الذي سيأتي بعد الهاتف الكفِّيِّ؟ يمكننا ربطُها أيضاً بـ **Musk**، فهو يتكلم عن **Neural ink** الذي كان يعملُ عليه **Musk** وهي عبارةٌ عن شريحةٍ إلكترونيةٍ تُزرع قريباً من جهة المخِ، لا

نفهم فيها كثيراً، ولكن فيها مشكلاتٌ من ناحيةٍ أخلاقيةٍ ونَظامِيَّةٍ لا بدَّ أن تُبحَثَ، المفروض أنه لا يُمنَعُ، ولكن دائماً لا بدَّ أن تبدأ من إدارة واعية تبحَثُ في مدى تفعِيلِهِ، وقابلِيَّتِهِ، وأخلاقيَّاتِهِ، وهل هو مناسب؟ وكيف من الممكن أن يُقنَّنَ ويُشرَّع؟ الآن هو تحت التطوير، لنفترض - على سنتين، ليس أشهراً، على سنتين قادمتينِ، أن هناك إمكانية أن تصدر **Technology** مثل هذا. فمن الآن، لا بدَّ أن تبدأ الإدارات الحكومية عندنا بالالتفاتِ له وتُجهِّز القوالب التشريعيةَ التي تكون مناسبةً له؛ لأنَّهُ أمرٌ سيصبحُ كبيراً لو أُطلِقَ في بداية الأمرِ، وبالتأكيدِ لن يكون للعامَّةِ مثلما أُطلِقَ الجوال، سيصبحُ لِفئاتٍ مُتخصِّصةٍ، وشيئاً فشيئاً يبدأ، إذا بدأت التقنية تنضج أكثر وأكثر، وتظهرُ مشاكلُها، وتظهرُ عيوبُها، فتبدأ بالتوسُّعِ، ويبدأ انتشارها يتوسع فيما بعد.

التدريب للوعي بالهجماتِ الإلكترونيةِ

بلا شك هذا أمر مُهم جداً، وأظن بعض الجهات بدأت بذلك ، مثل البنك المركزي بالتنسيق مع البنوك، فحملة «كُنْ نَبِيهاً» وغيرها كثير، وهذه التوعية ضروريةٌ ومُهمة، ودور المحاضرات والندوات كبيرٌ بلا شك؛ فَعامِلُ التوعية عاملٌ مُهمٌ، ويجب ألّا نملَّ منه وأن نحرص أن يكون على عِدَّةِ مستويات للتقني المتخصصُ، وعلى مستوى العامَّةِ

كنوع من التحذيراتِ، أو التنبيهاتِ في المجال. ونتمنى تبنّي حملاتٍ توعويةٍ تُبَثُّ عن طريق إعلانات أو نحوِ ذلك إذا وجدت الداعم لها إن شاء الله تعالى، والتوعية المفروض أن تبدأ من المدارسِ، وأن يُدرَجُ في المناهج بشكلٍ أكثر وأكثر ونبدأ بِتَدرِيسِهِ وبِتَعلِيمِهِ كأنه قِيَمٌ أخلاقِيَّةٌ، فمثلما نُعلِّمُهُ هذا الحلال وهذا الحرام، هذا يصلح، وهذا خطأ، أيضاً لا بدَّ أن أبدأ بِتَثقِيفِهِ في الأمن السيبراني ليدرك ما له وما عليه.

خاتمة:

إنّ الرحلة نحو الرقمنة الشاملة ليست مجرد سباق تقني نحو الأسرع أو الأحدث، بل هي عملية صياغة جديدة للحضارة الإنسانية في فضائها السيبراني، ولقد تبين لنا من خلال استعراض واقع التطور الرقمي وحماية المعلومات أنّ الأمن والابتكار هما وجهان لعملةٍ واحدة؛ فلا يمكن لابتكار تقني أن يستمر ويؤتي ثماره ما لم يستند إلى جدار صلب من الحماية والخصوصية، ولا يمكن لنظم الحماية أن تصمد ما لم تكن هي الأخرى متطورةً ومواكبةً لذكاء التهديدات المتجددة.

لقد أثبتت التجربة العالمية أنّ الفجوة الرقمية بين الدول لم تعد تقاس فقط بمدى توفر الإنترنت، بل بمدى القدرة على إدارة المخاطر الرقمية وحماية تدفق البيانات التي أصبحت شريان الحياة للاقتصاد الحديث. وفي هذا السياق، تبرز المملكة العربية السعودية كقصة نجاح استثنائية؛ حيث لم تكتفِ بتبني التقنية، بل وطنتها وحصنتها، محولةً التحديات الأمنية إلى فرص للاستثمار في الكوادر الوطنية وبناء صناعة أمن سيبراني منافسةٍ عالمياً، إنّ نجاح المملكة في الموازنة بين طموحات «رؤية ٢٠٣٠» وبين متطلبات السيادة الرقمية يبعث برسالة واضحة للعالم: أن التطور الرقمي السريع لا يعني بالضرورة التضحية بالأمان.

إننا نقف اليوم على أعتاب مرحلةٍ جديدةٍ تتلاشى فيها الحدود بين الواقع والافتراض، ممّا يفرض علينا جميعاً -أفراداً ومؤسسات ودولاً- أن نكون على قدر هذه المسؤولية؛ فالتحول الرقمي الذي نعيشه هو أعظم فرصةٍ في تاريخ البشرية للابتكار والنمو، وبقدر ما ننجح في حماية معلوماتنا، بقدر ما نضمن مستقبلاً أكثر ازدهاراً واستقراراً للأجيال القادمة.

* * * * *