المسؤولية القانونية لمقدمي الخدمات

عن جرائم أمن المعلومات في الدول العربية:

د. محمود فوزي

كبير خبراء استدامة التحول الرقمي لقطاع الاقتصاد الموجة

الوحدة الأولى: مقدمة عن العالم الرقمي وجرائم أمن المعلومات

1.1 المفاهيم الأساسية

مقدمو الخدمات الرقمية:

هم الشركات التي توفر خدمات الإنترنت، الهواتف المحمولة، التطبيقات، أو الخوادم (Servers) التي تخزن بياناتك.

- **مثال يومي:**
  - شركة **زين** في السعودية توفر الإنترنت للهواتف والمنازل. إذا اشتركت في خط إنترنت من زين، فهم مسؤولون عن حماية بياناتك (مثل رقم هاتفك أو عنوانك).
  - شركة **WE** في مصر تدير شبكات الإنترنت المنزلي، وهي مسؤولة عن حماية بيانات عملائها.
  - شركة **Ooredoo** في قطر تقدم خدمات السحابة (Cloud Services) التي تخزن بيانات الشركات.

جرائم أمن المعلومات:

هي أفعال غير قانونية تتم عبر الإنترنت أو الأجهزة، مثل:

- **سرقة البيانات**: مثل سرقة أرقام بطاقاتك البنكية من تطبيق تسوق.
- **الاحتيال**: إرسال رسائل بريد إلكتروني مزيفة تطلب منك كلمة المرور.
- **نشر محتوى غير قانوني**: مثل مواقع تدعم أفكارًا متطرفة.
- **مثال يومي**: تخيّل أنك تستخدم تطبيق "طلبات" لتوصيل الطعام، وفجأة يتم اختراق التطبيق وسرقة بيانات بطاقتك البنكية. هذه جريمة معلوماتية حدثت في الأردن عام 2020، حيث تم تسريب بيانات أكثر من 100,000 مستخدم بسبب ثغرة في الخادم (المصدر: تقرير الأمن السيبراني الأردني، 2020).

مسؤولية مقدمي الخدمات:

إذا أهملت الشركة حماية بياناتك (مثل عدم تحديث أنظمة الحماية)، فهي مسؤولة قانونيًا وقد تُعاقب بغرامات أو دعاوى قضائية.

- **مثال تفصيلي:**

في 2019، تعرضت شركة **Etisalat** في الإمارات لخرق أمني بسبب عدم تحديث برمجياتها الأمنية. تم تسريب بيانات آلاف العملاء، مما أدى إلى غرامة من هيئة تنظيم الاتصالات الإماراتية ودعاوى من العملاء المتضررين (المصدر: تقرير هيئة تنظيم الاتصالات الإماراتية، 2019).

- **مثال آخر**: إذا اشتركت في خدمة إنترنت منزلي من **STC** في السعودية، وتم اختراق بياناتك بسبب إهمالهم في استخدام "جدار ناري"، يمكن أن تُقاضي الشركة.

1.2 تطور البيئة القانونية والتقنية

التطور القانوني:

الدول العربية تحاول تحديث قوانينها لمواجهة الجرائم الإلكترونية، لكنها تواجه تحديات بسبب سرعة تطور التكنولوجيا.

- **مثال في الإمارات**: في 2021، أُدخلت قوانين جديدة لمعاقبة من يستخدم الذكاء الاصطناعي في الاحتيال، مثل إنشاء فيديو مزيف (Deepfake) لخداع البنوك (المصدر: قانون مكافحة الجرائم الإلكترونية الإماراتي، 2021).
- **مثال في السعودية**: نظام حماية البيانات الشخصية (2021) يطالب الشركات بحماية بيانات العملاء، مثل عناوينهم أو أرقام حساباتهم البنكية (المصدر: الهيئة السعودية للبيانات والذكاء الاصطناعي، 2021).
- **مثال في الأردن**: بعد زيادة هجمات "Phishing" (رسائل احتيالية) في 2023، أصدر البنك المركزي الأردني تعليمات للبنوك لتحسين حماية المعاملات الرقمية (المصدر: تقرير البنك المركزي الأردني، 2023).

التحديات:

- القوانين العربية غالبًا لا تستطيع مواكبة أساليب القراصنة الجديدة، مثل هجمات "Ransomware" التي تُشفّر بياناتك وتطالب بفدية.
- نقص الخبراء التقنيين في الشرطة أو القضاء لفهم هذه الجرائم.
- **مثال يومي**: إذا تلقيت رسالة واتساب تدّعي أنها من بنكك وتطلب كلمة المرور، هذا هجوم "Phishing". في مصر، زادت هذه الهجمات في 2022، مما دفع الحكومة لإطلاق حملات توعية (المصدر: تقرير الأمن السيبراني المصري، 2022).

1.3 دراسات حالة (عالمية)

1. **فيسبوك وCambridge Analytica (2018)**:
   - **القصة**: شركة Cambridge Analytica استخدمت بيانات 87 مليون مستخدم من فيسبوك دون إذنهم للتأثير على حملات سياسية.
   - **لماذا حدث؟**: فيسبوك لم يضع قواعد صارمة لحماية بيانات المستخدمين من الأطراف الثالثة.
   - **النتيجة**: دفع فيسبوك غرامة 5 مليارات دولار للجنة التجارة الفيدرالية الأمريكية (FTC)، واضطر لتحسين أنظمة الحماية (المصدر: تقرير FTC، 2019).
   - **الدرس**: الشركات الكبرى مسؤولة عن حماية بياناتك حتى لو كانت تتعامل مع شركات أخرى.
2. **Amazon Web Services (AWS) (2020)**:
   - **القصة**: استضافت AWS مواقع تحتوي على محتوى غير قانوني (مثل خطاب الكراهية).
   - **لماذا حدث؟**: AWS لم تراقب المحتوى جيدًا في البداية.

- **النتيجة**: بعد انتقادات، حدّثت AWS سياساتها لمنع استضافة محتوى غير قانوني (المصدر: تقرير Southern Poverty Law Center، 2020).
- **الدرس**: شركات الاستضافة السحابية مسؤولة عن مراقبة ما يُنشر على خوادمها.

3. **Equifax (2017)**:
   - **القصة**: تم اختراق بيانات 147 مليون شخص (مثل أرقام الضمان الاجتماعي) بسبب ثغرة في برنامج قديم (Apache Struts).
   - **لماذا حدث؟**: Equifax لم تحدث أنظمتها الأمنية في الوقت المناسب.
   - **النتيجة**: دفعت الشركة 700 مليون دولار كتعويضات، وأُجبرت على تحسين أنظمتها (المصدر: تقرير FTC، 2019).
   - **الدرس**: تحديث البرامج بانتظام ضروري لمنع الاختراقات.

4. **SolarWinds (2020)**:
   - **القصة**: هجوم إلكتروني استهدف شركة SolarWinds، مما سمح للقراصنة بالوصول إلى بيانات شركات وحكومات عالمية.
   - **لماذا حدث؟**: ثغرة في برنامج إدارة الشبكات لم تُكتشف في الوقت المناسب.
   - **النتيجة**: أثر الهجوم على آلاف الشركات، ودفع SolarWinds لتحسين أنظمة الأمان (المصدر: تقرير FireEye، 2020).
   - **الدرس**: حتى الشركات الكبرى يمكن أن تُخترق إذا أهملت الحماية.

الوحدة الثانية: القوانين العربية ومسؤولية الشركات

2.1 تحليل القوانين الوطنية

1. **مصر**:
   - قانون مكافحة الجرائم الإلكترونية (2018) يطالب شركات الإنترنت بحفظ بيانات المستخدمين (مثل سجل تصفحك) لمدة 180 يومًا، وتسليمها للشرطة إذا طُلب ذلك.
   - **مثال يومي**: إذا استخدم شخص تطبيق "واتساب" للاحتيال، يمكن للشرطة طلب بياناته من شركة الإنترنت.
   - **دراسة حالة**: في 2018، تعرض تطبيق **Careem** لاختراق أدى إلى تسريب بيانات 14 مليون مستخدم. التحقيقات كشفت أن الشركة لم تتبع قواعد الحماية بشكل كامل، مما أثار جدلًا قانونيًا (المصدر: تقرير Cybersecurity Egypt، 2018).
2. **السعودية**:
   - نظام مكافحة جرائم المعلوماتية (2007) يعاقب مرتكبي الجرائم الإلكترونية بغرامات تصل إلى 5 ملايين ريال أو السجن 7 سنوات، لكنه غير واضح بشأن مسؤولية الشركات.
   - **مثال يومي**: إذا تم اختراق حسابك البنكي بسبب إهمال مزود الإنترنت، القانون قد لا يحدد بوضوح من المسؤول.
   - **دراسة حالة**: هجوم **Shamoon** عام 2012 على شركة أرامكو دمر آلاف الحواسيب بسبب فيروس، وكشف عن ضعف أنظمة الحماية لدى مزودي الخدمات (المصدر: تقرير FireEye، 2012).

3. **الإمارات:**
   - قانون مكافحة الجرائم الإلكترونية (2021) يفرض غرامات تصل إلى 500,000 درهم على الشركات التي تهمل حماية بيانات العملاء، ويطالبها بالتعاون الفوري مع الشرطة.
   - **مثال يومي:** إذا اشتريت من موقع "نون" وتم اختراق بياناتك، يجب على الشركة إبلاغ الشرطة فورًا.
   - **دراسة حالة:** في 2020، تم اختراق موقع **نون** بسبب ثغرة في خادم الاستضافة، وتم تغريم مزود الخدمة لعدم تحديث أنظمته (المصدر: تقرير هيئة تنظيم الاتصالات، 2020).
4. **الأردن:**
   - قانون الجرائم الإلكترونية (2015) يطالب مزودي الخدمات بحماية بيانات العملاء والتعاون مع الجهات الأمنية.
   - **دراسة حالة:** في 2021، تم اختراق موقع حكومي أردني بسبب ضعف حماية الخادم، وأُلزمت الشركة المستضيفة بتحسين أنظمتها (المصدر: تقرير الأمن السيبراني الأردني، 2021).

2.2 حدود المسؤولية

- **مسؤولية مباشرة:** إذا تسببت الشركة عن عمد أو إهمال في جريمة، مثل السماح بنشر محتوى غير قانوني.
  - **مثال يومي:** إذا سمح مزود إنترنت بنشر إعلانات احتيالية على موقعه بسبب عدم المراقبة، فهو مسؤول.
  - **دراسة حالة:** في السعودية (2022)، تم تغريم شركة استضافة لأنها سمحت بنشر محتوى إرهابي على موقع مستضاف بسبب ضعف أنظمة الرصد (المصدر: تقرير هيئة الاتصالات السعودية، 2022).
- **مسؤولية غير مباشرة:** إذا أهملت الشركة حماية بياناتك دون قصد.

- **مثال يومي**: إذا لم تستخدم شركة إنترنت تشفيرًا قويًا (مثل HTTPS)، وتم اختراق بياناتك، فهي مسؤولة عن الإهمال.
- **دراسة حالة**: في مصر (2021)، تم اختراق متجر إلكتروني بسبب عدم تفعيل أنظمة إنذار أمنية، مما أدى إلى سرقة بيانات آلاف العملاء (المصدر: تقرير الأمن السيبراني المصري، 2021).

2.3 دراسات حالة (محلية)

1. **الإمارات (2020)**:
   - **القصة**: موقع تجاري تم اختراقه بسبب ضعف حماية الخادم المستضاف.
   - **لماذا حدث؟**: مزود الاستضافة لم يحدث برمجياته الأمنية.
   - **النتيجة**: تم تغريم المزود وإلزامه بدفع تعويضات للعملاء المتضررين (المصدر: تقرير هيئة تنظيم الاتصالات، 2020).
2. **مصر (2022)**:
   - **القصة**: منصة **طلبات** تعرضت لاختراق أدى إلى سرقة بيانات بطاقات دفع العملاء.
   - **لماذا حدث؟**: ضعف أنظمة الحماية في الخادم المستضاف.
   - **النتيجة**: التحقيقات أظهرت إهمال مزود الخدمة، مما أدى إلى تحسين القوانين المحلية (المصدر: تقرير الأمن السيبراني المصري، 2022).
3. **السعودية (2023)**:
   - **القصة**: هجوم "Ransomware" استهدف شركة حكومية، حيث شُفّرت بياناتها وطُلبت فدية.
   - **لماذا حدث؟**: مزود الخدمة السحابية لم يستخدم أنظمة حماية قوية.
   - **النتيجة**: تحديث نظام حماية البيانات الشخصية ليشمل قواعد صارمة للمزودين (المصدر: تقرير الهيئة الوطنية للأمن السيبراني، 2023).
4. **البحرين (2022)**:

- **القصة**: اختراق موقع بنكي بسبب هجوم "Phishing" استهدف عملاء البنك عبر رسائل بريد إلكتروني مزيفة.
- **لماذا حدث؟**: مزود البريد الإلكتروني لم يستخدم أنظمة تصفية قوية.
- **النتيجة**: أصدرت هيئة الاتصالات تعليمات جديدة لتحسين الحماية (المصدر: تقرير هيئة تنظيم الاتصالات البحرينية، 2022).

الوحدة الثالثة: القوانين الدولية ومقارنتها

3.1 تشريعات الاتحاد الأوروبي

- **اللائحة العامة لحماية البيانات (GDPR)**:
  - يطالب الشركات بالإبلاغ عن أي اختراق خلال 72 ساعة، وإلا تُعاقب بغرامات ضخمة.
  - **مثال يومي**: إذا تم اختراق موقع مثل Booking.com، يجب أن يُبلغ العملاء والحكومة فورًا.
  - **دراسة حالة**: في 2020، عوقبت **Booking.com** في هولندا بغرامة 475,000 يورو لتأخرها في الإبلاغ عن خرق أمني أثر على بيانات العملاء (المصدر: تقرير هيئة حماية البيانات الهولندية، 2020).
- **توجيه الأمن السيبراني (NIS)**:
  - يطالب شركات الإنترنت الكبرى بحماية قوية واستجابة سريعة للهجمات.
  - **مثال يومي**: إذا تعرضت شركة إنترنت لمحاولة اختراق، يجب أن يكون لديها خطة جاهزة للتصدي.

- **دراسة حالة**: في 2019، تعرضت شركة طيران أوروبية (British Airways) لاختراق، مما دفع مزودي الخدمات لتحسين أنظمة الرصد (المصدر: تقرير ENISA، 2019).

3.2 التشريعات الأمريكية

- **قانون CLOUD Act (2018)**:
  - يسمح للحكومة الأمريكية بطلب بيانات من شركات الإنترنت حتى لو كانت مخزنة خارج أمريكا.
  - **مثال يومي**: إذا استخدمت خدمة مثل Google Drive، يمكن للحكومة الأمريكية طلب بياناتك حتى لو كنت في بلد آخر.
  - **دراسة حالة**: في 2018، رفضت **مايكروسوفت** تسليم بيانات مخزنة في أيرلندا، مما تسبب في نزاع قانوني مع الحكومة الأمريكية (المصدر: تقرير Microsoft، 2018).
- **قانون حماية الاتصالات الإلكترونية (ECPA)**:
  - يحمي بياناتك من التجسس غير القانوني.
  - **دراسة حالة**: في 2016، تم اختراق 500 مليون حساب في **Yahoo** بسبب ضعف أنظمة الحماية، مما أثار تساؤلات حول التزامها بقانون ECPA (المصدر: تقرير Verizon، 2017).

3.3 توافقيات دولية

- **اتفاقية بودابست (2001)**:
  - هي اتفاقية عالمية تشجع الدول على وضع قوانين لمحاربة الجرائم الإلكترونية، وتطالب الشركات بحفظ بيانات المستخدمين لمساعدة الشرطة.
  - **مثال يومي**: إذا ارتكب شخص جريمة عبر الإنترنت في الأردن، يمكن للشرطة طلب مساعدة من دول أخرى بفضل هذه الاتفاقية.

- **دراسة حالة**: انضمت الأردن للاتفاقية في 2007، مما ساعد في تعقب مجرمين عبر الحدود (مثل قضايا الاحتيال الإلكتروني) (المصدر: تقرير مجلس أوروبا، 2007).

3.4 دراسة مقارنة

- **نقاط قوة الغرب**:
  - قوانين واضحة تحدد مسؤوليات الشركات (مثل GDPR).
  - حماية قوية لخصوصية المستخدمين.
  - أنظمة إبلاغ سريعة عن الخروقات.
- **نقاط ضعف الدول العربية**:
  - القوانين تختلف من بلد لآخر، مما يسبب ارتباكًا.
  - نقص الخبراء التقنيين في القضاء والشرطة.
  - ضعف التنسيق بين الدول العربية لمكافحة الجرائم الإلكترونية.

الوحدة الرابعة: الأبعاد التكنولوجية للمسؤولية

4.1 الجانب التقني للمسؤولية

لماذا تحدث الجرائم الإلكترونية؟

تحدث بسبب أخطاء تقنية مثل:

- **عدم تشفير البيانات**: مثل استخدام موقع غير آمن (بدون HTTPS).
- **برامج قديمة**: عدم تحديث أنظمة الحماية يفتح الباب للقراصنة.
- **عدم وجود جدار ناري (Firewall)**: مثل عدم وجود قفل على باب منزلك الرقمي.

مثال يومي:

إذا اشتريت من موقع لا يستخدم HTTPS (سترى رمز القفل مفقودًا في المتصفح)، فبياناتك مثل رقم بطاقتك البنكية قد تُسرق بسهولة.

دراسة حالة:

في قطر (2022)، تعرضت شركة تقنية لاختراق عبر هجوم "SQL Injection" (وهو نوع من الهجمات يستهدف قواعد البيانات) بسبب عدم تحديث برمجياتها، مما أدى إلى سرقة بيانات العملاء (المصدر: تقرير الأمن السيبراني القطري، 2022).

4.2 الأدلة الرقمية

ما هي الأدلة الرقمية؟

هي المعلومات التي تساعد في تعقب المخترقين، مثل:

- **سجلات الدخول (Logs)**: توضح من دخل إلى الموقع ومتى.
- **عناوين IP**: تُظهر موقع الجهاز الذي نفّذ الهجوم.
- **سجلات الخادم**: تُظهر الأنشطة على الخادم (مثل من حاول اختراقه).

مثال يومي:

إذا حاول شخص اختراق حسابك البنكي، يمكن للبنك معرفة من أين جاء الهجوم باستخدام عنوان IP.

دراسة حالة:

في الأردن (2021)، تم تعقب مخترق لنظام حكومي باستخدام سجل الدخول إلى الخادم (Server Access Log)، مما ساعد في القبض عليه (المصدر: تقرير الأمن السيبراني الأردني، 2021).

4.3 دراسات حالة

1. **مصر (2021):**
   - **القصة**: تم اختراق نظام حكومي بسبب هجوم "DDoS" (يُغرق الموقع بزوار مزيفين لتعطيله).
   - **لماذا حدث؟**: مزود الخدمة لم يكن لديه أنظمة رصد قوية.
   - **النتيجة**: أُلزمت الشركة بتحسين أنظمتها، وأُدخلت قواعد جديدة للرصد (المصدر: تقرير الأمن السيبراني المصري، 2021).
2. **السعودية (2022):**
   - **القصة**: هجوم "Phishing" استهدف عملاء بنك عبر رسائل بريد إلكتروني مزيفة.
   - **لماذا حدث؟**: مزود البريد الإلكتروني لم يستخدم أنظمة تصفية قوية.
   - **النتيجة**: تحديث سياسات الأمن السيبراني لتشمل تدقيق مزودي الخدمات (المصدر: تقرير الهيئة الوطنية للأمن السيبراني، 2022).
3. **الكويت (2023):**
   - **القصة**: اختراق تطبيق تسوق بسبب ثغرة في قاعدة البيانات، مما أدى إلى سرقة بيانات العملاء.
   - **لماذا حدث؟**: المزود لم يستخدم تشفيرًا قويًا.
   - **النتيجة**: فرضت هيئة الاتصالات قواعد جديدة لتشفير البيانات (المصدر: تقرير هيئة تنظيم الاتصالات الكويتية، 2023).

الوحدة الخامسة: رؤية مستقبلية ونموذج تشريعي مقترح

5.1 التحديات القادمة

- **الذكاء الاصطناعي:**
  - يُستخدم في هجمات متطورة، مثل تزييف الأصوات أو الفيديوهات (Deepfake) لخداع البنوك أو الأفراد.
  - **مثال يومي:** تخيّل أنك تتلقى مكالمة من شخص يدّعي أنه مديرك، لكن الصوت مزيف باستخدام الذكاء الاصطناعي.
  - **دراسة حالة:** في 2020، استخدم قراصنة تقنية Deepfake لتزييف صوت مدير تنفيذي في الإمارات، مما أدى إلى سرقة 35 مليون دولار (المصدر: تقرير Forbes، 2021).
- **البلوكشين:**
  - تقنية مثل العملات الرقمية (بيتكوين) قد تُستخدم في الاحتيال إذا لم تُنظم.
  - **مثال يومي:** إذا اشتريت عملات رقمية من منصة غير منظمة، قد تُسرق أموالك.
  - **دراسة حالة:** في 2021، تم اختراق منصة **Poly Network** وسرقة 600 مليون دولار من العملات الرقمية بسبب ثغرة في العقود الذكية (المصدر: تقرير Chainalysis، 2021).

5.2 ملامح نموذج عربي مقترح

اقتراحات تشريعية:

1. وضع قواعد واضحة لمسؤولية الشركات (مثل تحديث الأنظمة بانتظام).
2. إضافة قوانين لتنظيم استخدام الذكاء الاصطناعي والبلوكشين.
3. إنشاء موقع إلكتروني عربي موحد للإبلاغ عن الخروقات.

4. مطالبة الشركات بالإبلاغ عن أي اختراق خلال 48 ساعة، مثل قانون GDPR الأوروبي.

مثال يومي:

إذا أُجبرت الشركات على الإبلاغ عن الاختراقات خلال 48 ساعة، يمكن للشرطة التصرف بسرعة لمنع المزيد من الضرر.

5.3 التوصيات

1. تحديث القوانين كل 3-5 سنوات لمواكبة التكنولوجيا.
2. إنشاء هيئة عربية مشتركة للأمن السيبراني لتبادل المعلومات بين الدول.
3. تدريب القضاة والشرطة على فهم الأدلة الرقمية، مثل كيفية قراءة سجلات الخادم.