# الخصوصية وحماية البيانات

# قرارك يحمي مؤسسة كاملة

PROTECTING YOUR DIGITAL FUTURE

نبيل العبيـــدي



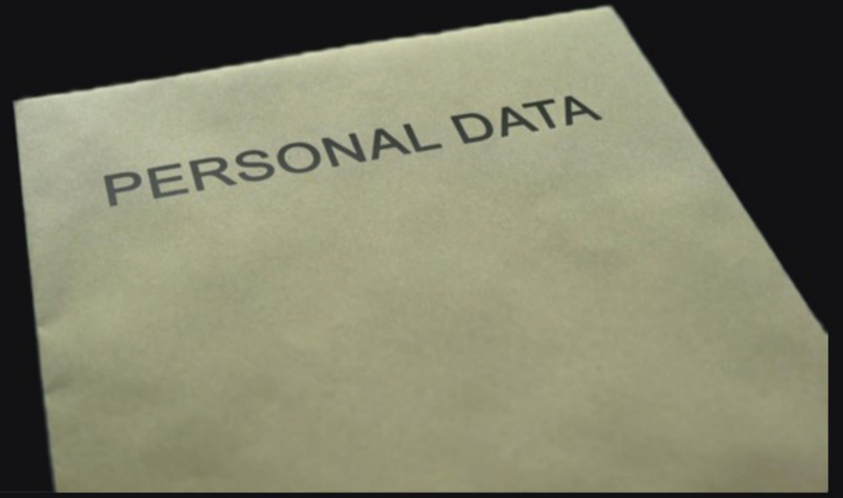
هل تعلمون أن هناك من يعرف الآن

- أين جلستم هذا الصباح
- ماذا اشتريتم قبل قليل
- وحتى عدد خطواتكم منذ استيقاظكم


كل يوم يُباع شيء منكم دون أن تشعروا...

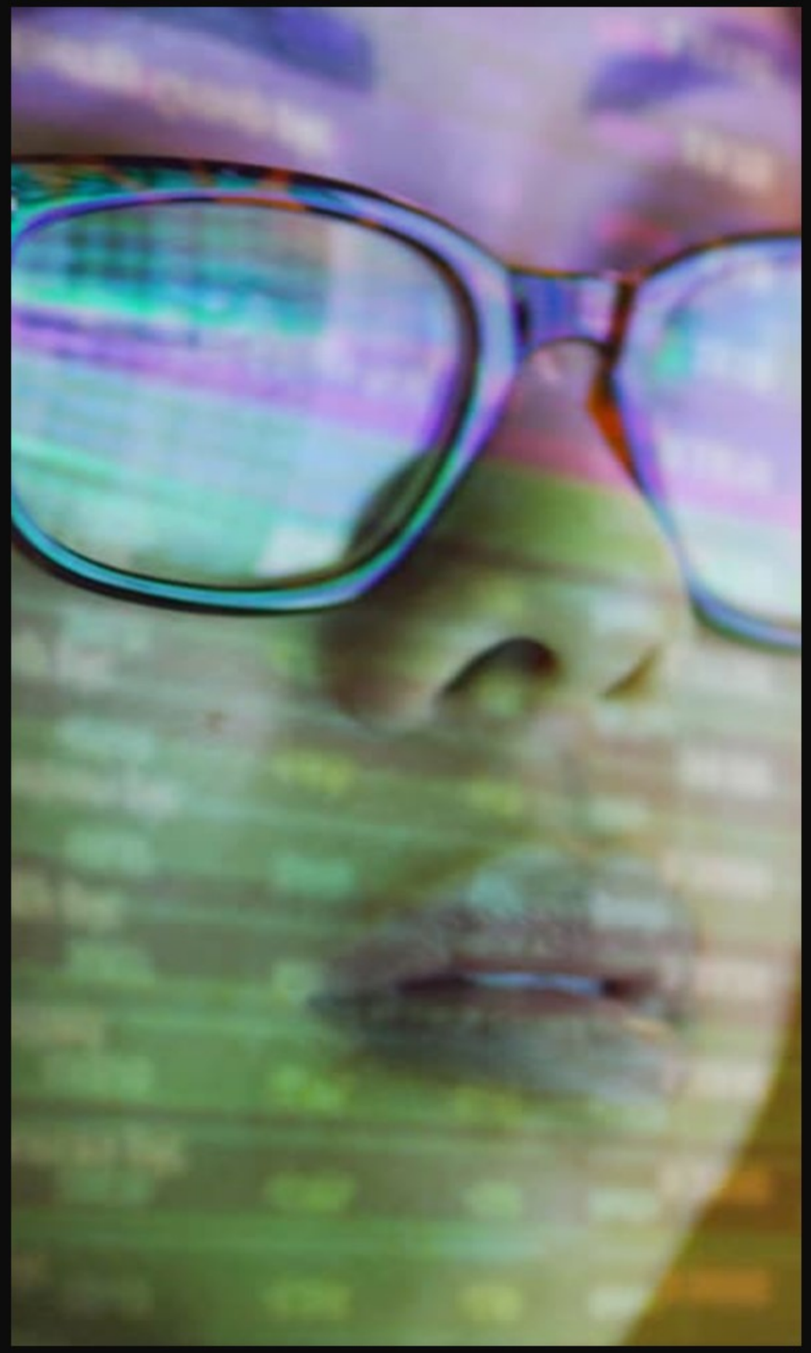
هذه ليست مبالغة: هناك سوق مظلم للبيانات
يدرّ تريليونات الدولارات سنويًا.

تخيلوا أن ملفًا بسيطًا يحوي بياناتكم الشخصية
يتسرب على شبكة الإنترنت المظلم خلال ثوانٍ...
تخيلوا أن هذا الملف يباع، ويصل إلى من يريد استغلاله.



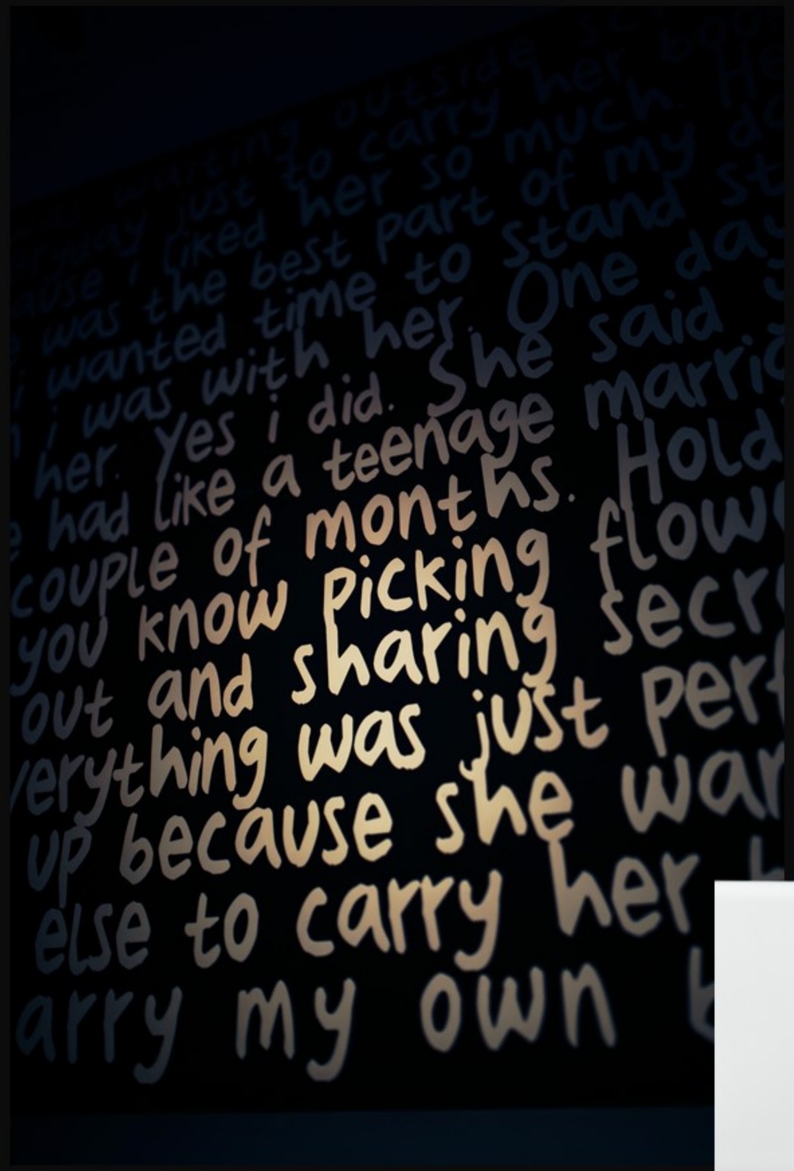
إذا كان تسريب البيانات اليوم
خطرًا، فالغد أخطر.

نحن على أعتاب عصر تُعامل
فيه البيانات كوقود استراتيجي
يفوق قيمة النفط.



تسريب بيانات ملايين الحسابات في منصات عالمية،

واختراق بيانات بطاقات ائتمان في كبرى البنوك، ... كلها أمثلة حقيقية.




# التكنولوجيا قد تكون حصناً منيعاً، لكن ثغرة واحدة تبدأ من

**موظف غير منتبه**

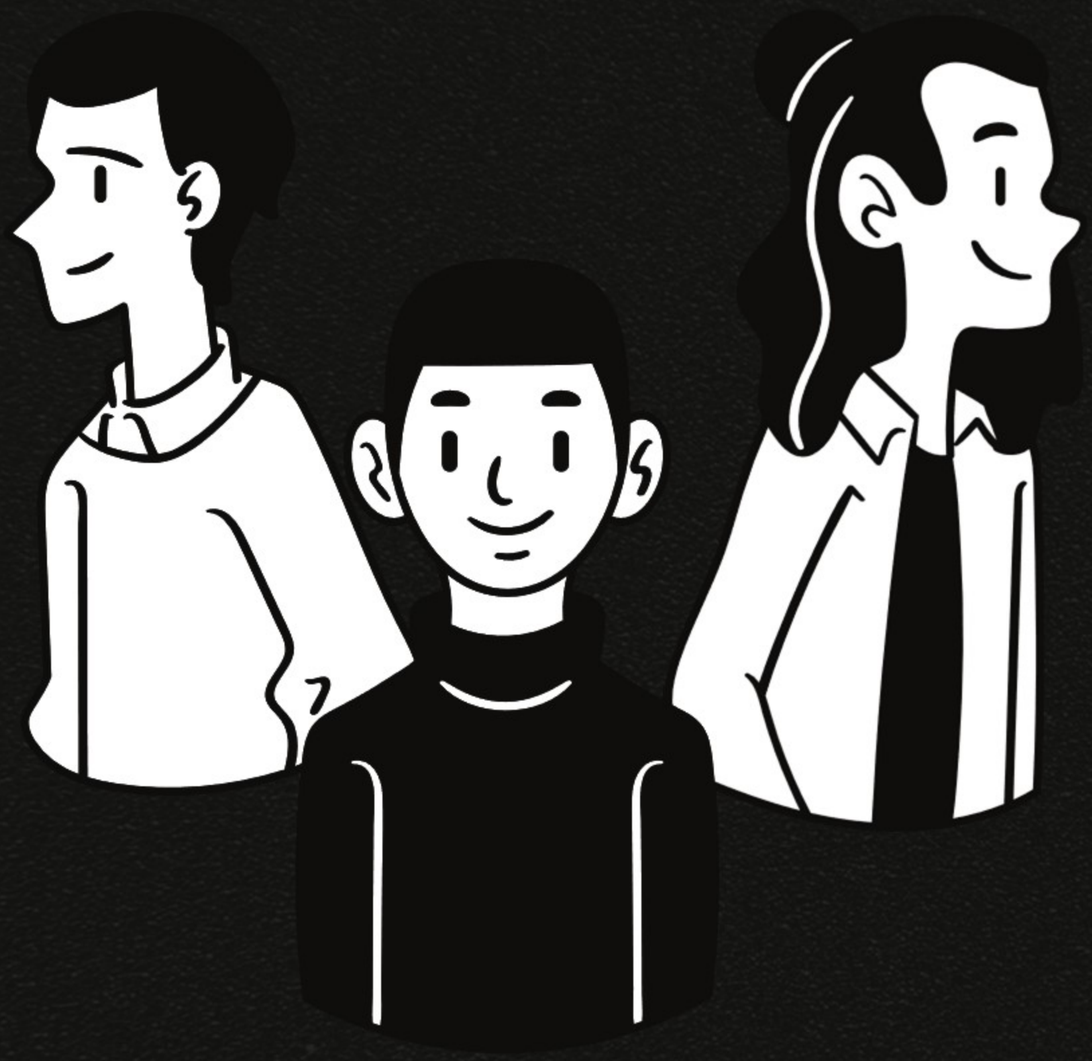
# لمحة تاريخية عن حماية البيانات (عالمياً)

| | | |
|---|---|---|
| **السبعينيات** | مع بدايات الحواسيب المركزية ظهرت أولى المخاوف حول استخدام البيانات الشخصية | عام 1970 أصدرت ولاية هِسّن الألمانية أول قانون لحماية البيانات في العالم، تبعتها ألمانيا الاتحادية ثم السويد عام 1973 بقوانين مماثلة |
| **الثمانينات (أعتراف دولي)** | في 1980 أقرّت منظمة التعاون الاقتصادي والتنمية (OECD) مبادئ الخصوصية أصبحت مرجعًا عالميًا | هذه المبادئ وضعت أساس: جمع البيانات لغرض محدد، والحصول على موافقة الأفراد |

| | | |
|---|---|---|
| **التسعينيات (عصر الأنترنت)** | انفجار الشبكة العنكبوتية جعل البيانات تنتقل بلا حدود | الاتحاد الأوروبي أصدر أول توجيه شامل لحماية البيانات عام 1995، واضعًا قاعدة "الموافقة الصريحة" |
| **الألفية الجديدة (الهجمات الكبري)** | فضائح مثل تسريبات ياهو وسرقة بطاقات الأتمان دفعت الحكومات لتشديد القوانين | ظهرت قوانين كقانون حماية خصوصية المستهلك في كاليفورنيا (CCPA) .. وبدأ الحديث عن الأمن السيبراني على مستوى عالمي |

| | | |
|---|---|---|
| **نقلة نوعية 2018** | اللائحة الأوروبية العامة لحماية البيانات (GDPR) دخلت حيز التنفيذ | وأصبحت المعيار العالمي الأقوى، بفرضها غرامات ضخمة تصل إلى 4٪ من الإيرادات السنوية لأي شركة |
| **المرحلة الراهنة (البيانات كسلاح استراتيجي)** | اليوم أصبحت حماية البيانات أمنًا وطنيًا لا يقل أهمية عن الأمن العسكري أو الاقتصادي | تسريبات كبرى مثل Cambridge Analytica أثبتت أن البيانات قادرة على التأثير في الانتخابات والاقتصادات |

# تطوّر مفهوم خصوصية الأفراد



# ما قبل العصر الرقمي

## خصوصية فطريه

# السبعينيات والثمانينيات

## بداية القلق

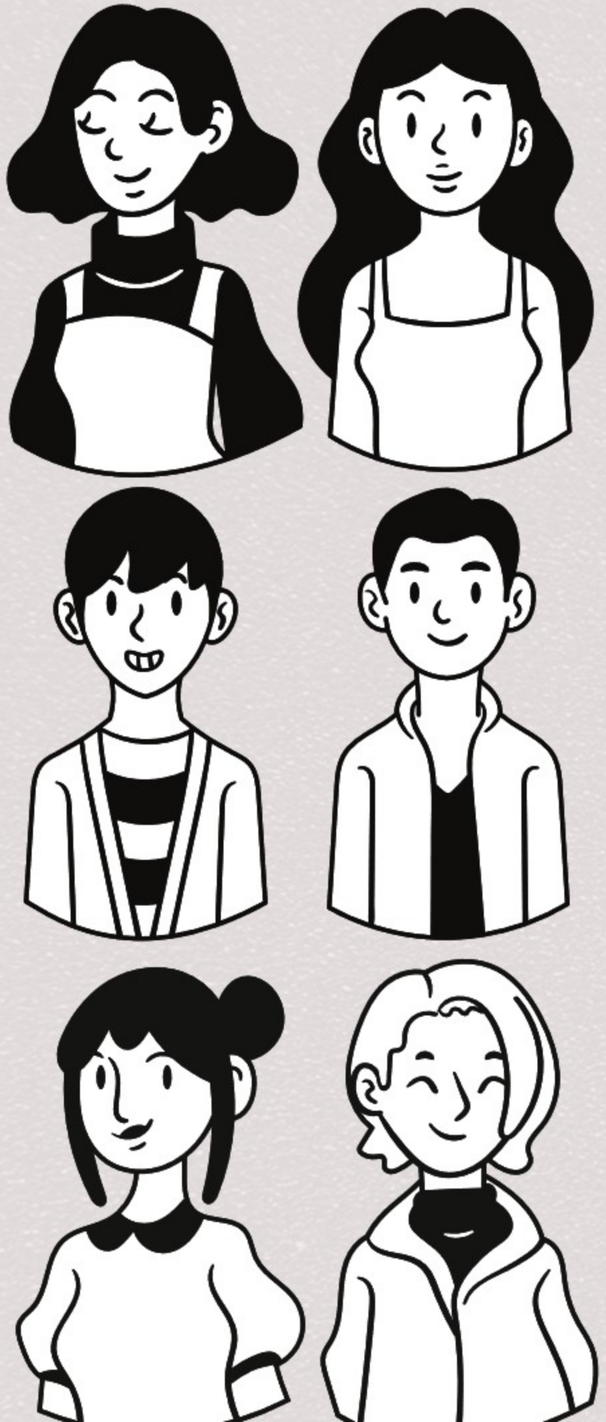
مع الحواسيب المركزية بدأت تظهر أول قواعد بيانات ضخمة عن المواطنين (السجلات الطلابية ، الطبية)
ظهرت فكرة أن المعلومة عن الشخص قد تُستخدم ضده حتى دون علمه

# التسعينيات

## صدمة الإنترنت

البريد الإلكتروني والتجارة الإلكترونية أدخلا الأفراد إلى فضاء رقمي مفتوح بدأنا نمنح بياناتنا طوعًا: أسماء ، عناوين ، أرقام بطاقات..

كثيرون لم يدركوا أن كل ضغطت زر تُسجل وتُخزن إلى الأبد



# الألفية الجديدة

## الشبكات الاجتماعية

مع صعود فيسبوك وتويتر  وغيرها صار الأفراد ينشرون طواعية أدق تفاصيل حياتهم

ظهرت أولى القضايا عن حق ملكية البيانات الشخصية

# العقد الأخير

# من المستخدم إلى "المنتَج"

الهواتف الذكية والتطبيقات حولت حياة الفرد إلى تيار بيانات

لحظي: الموقع، الصحة، النوم، المشتريات

**شركات كبرى بنت ثرواتها على تحليل هذه البيانات**

# العقد القادم

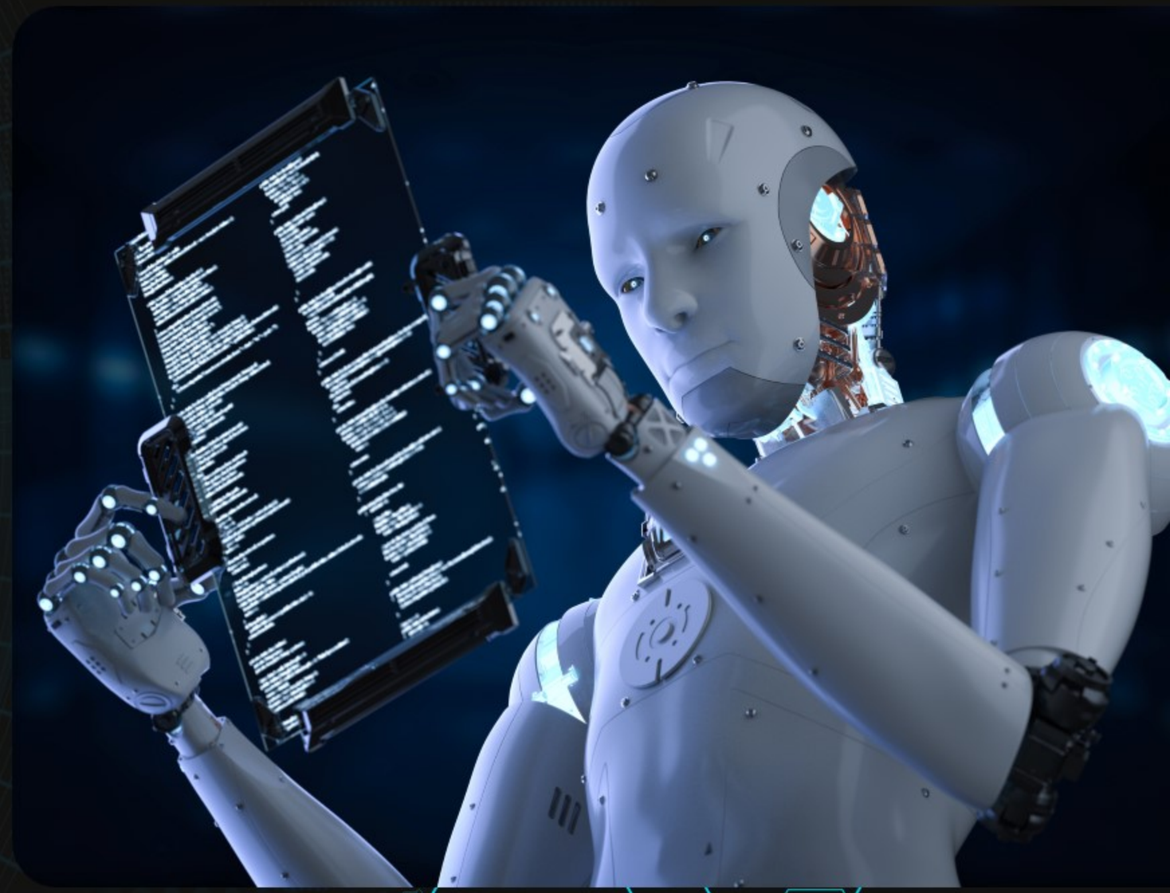
## تحديات الهوية الرقمية

هوية رقمية موحّدة قد تشمل سجلك المالي والصحي والاجتماعي

هجمات الانتحال العميق (Deepfake )
قد تخلق نسخا رقمية منك تتحدث وتتصرف مكانك

# لهذا

في نصف قرن انتقل الفرد من مالك كامل لبياناته إلى كائن تُصاغ قرارات حياته من خوارزميات لا يراها. هذه هي الثورة الصامتة التي نعيشها جميعًا




الحرب الرقمية
الخفية
تعطيل المؤسسات
لتعطيل القرارات و تأثير بالرأي العام


# تطور خصوصية البيانات في القطاع العام


## الأوراق المغلقة
## إلى
## الحوكمة الذكية للبيانات

# المرحلة الأولى: الإدارة الورقية (قبل التسعينيات)

- الاعتماد الكلي على الملفات المادية والمراسلات الورقية.
- حماية الخصوصية كانت "طبيعية" لأن البيانات غير رقمية.
- لم تكن هناك قوانين واضحة، بل تعليمات إدارية عامة مثل "سرية المراسلات الحكومية".

**كانت الخصوصية تعتمد على الأخلاق الوظيفية، لا على الأنظمة**

**نقص في الوعي القانوني بأهمية البيانات كأصل، وضعف في مفهوم المسؤولية الفردية تجاه تسريبها.**

**التحدي:**

# المرحلة الثانية: الميكنة والرقمنة الإدارية (التسعينيات – منتصف الألفية)

- بداية استخدام الحواسيب المركزية في الوزارات (مثل نظم الرواتب، والملفات الطبية).
- تبادل البيانات بين الجهات الحكومية بدأ يظهر لأول مرة عبر شبكات داخلية.
- ظهرت أولى سياسات حماية المعلومات الحساسة داخل الوزارات الدفاعية والمالية.
- التحدي:
- نقص في البنية التشريعية، وعدم وجود مفهوم موافقة المواطن على جمع بياناته.

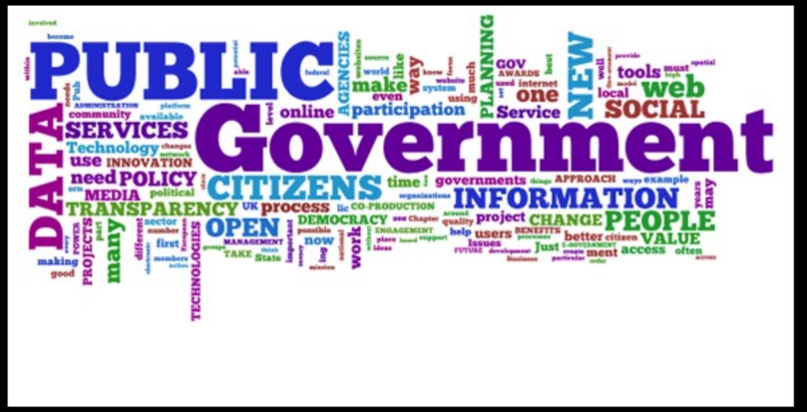
**كان التركيز على كفاءة النظام... وليس على أمن البيانات.**

# المرحلة الثالثة: الحكومة الإلكترونية (2005 – 2018) تقريبا

إطلاق بوابات حكومية موحدة للخدمات الإلكترونية.

تراكم بيانات ضخمة عن المواطنين (الهوية، التعليم، الصحة)

ظهور الوعي الأولي بضرورة تشريعات لحماية البيانات (تأثراً بالـ GDPR الأوروبي)




- التغير النوعي:
  - إنشاء إدارات "أمن معلومات" و"حوكمة بيانات" في بعض الجهات.
  - تطبيق مبادئ التصنيف المعلوماتي. (Public – Restricted – Confidential – Secret)
  - بدء مراقبة دخول المستخدمين وتسجيل العمليات. (Audit Trails)

**أنتقلنا من أدارة الملفات الى أدارة الثقة الرقمية**

# المرحلة الرابعة :التحول الرقمي الشامل (2019 – حتى اليوم)

**تكامل الأنظمة الحكومية في بيئات سحابية مركزية.**

**استخدام الذكاء الاصطناعي في تحليل البيانات الحكومية لاتخاذ القرار.**

**تبنّي مفهوم "البيانات الوطنية "كأصل سيادي.**

**التحدي الجديد.:**

- **ضرورة وجود إطار وطني لحوكمة البيانات** (National Data Governance Framework).

**الخصوصية لم تعد منع الوصول إلى البيانات ... بل ضبط استخدامها.**

**حماية الخصوصية لم تعد تقنية فقط، بل قانونية، سلوكية، وسياسية**


**تفعيل مبدأ المواطنة الرقمية الآمنة**
(Digital Citizenship).

# المرحلة القادمة رؤية مستقبلية حتى (2030)

هوية رقمية موحدة للمواطن والموظف ترتبط بالأمن السيبراني الوطني

تحليل لحظي لحركة البيانات الحكومية لكشف الأنشطة المشبوهة في الزمن الحقيقي.

"البيانات بالتصميم (Privacy by Design): "
أي أن كل نظام حكومي جديد يجب أن يبنى على أساس حماية الخصوصية من البداية.

منصات وطنية للشفافية :تتيح للمواطن معرفة من استخدم بياناته ومتى ولماذا.

ذكاء اصطناعي وطني حارس للبيانات الحكومية قادر على اكتشاف أنماط السلوك الإداري غير المصرح به.

# توجهات حديثة في خصوصية بيانات القطاع العام

التشريعات

الذكاء الأصطناعي

التحول الرقمي

الشفافية

حوكمة البيانات

الوعي الوظيفي

# توجهات حديثة في خصوصية بيانات القطاع العام (2025 وما بعد)

| المجال | الاتجاه الحالي | الاتجاه الاستراتيجي |
| --- | --- | --- |
| التشريعات | أصدار قوانين وطنية لحماية البيانات | لموائمة التوافق الدولي (GDPR) |
| التحول الرقمي | أنشاء مراكز بيانات سيادية وطنية | ضمان أن تبقي بيانات المواطنين داخل الدولة |
| حوكمة البيانات | تشكيل لجان عليا للبيانات الوطنية | توحيد السياسات والمعايير بين الجهات |

# توجهات حديثة في خصوصية بيانات القطاع العام (2025 وما بعد)

| المجال | الاتجاه الحالي | الاتجاه الاستراتيجي |
| --- | --- | --- |
| الذكاء الأصطناعي | أستخدام خوارزميات مراقبة الأستخدام الداخلي | أكتشاف أي أساءة أو تسريب مبكرا |
| الشفافية | تعزيز حق المواطن في معرفة أستخدام بياناته | تعزيز الثقة بين الحكومة والمجتمع |
| الوعي الوظيفي | أدراج التدريب الأمني ضمن تقييم الأداء الوظيفي | تحويل الوعي الرقمي الى سلوك/معيار مهني |

Future War

# أين تتجه حرب البيانات عالميا؟

# صعود الذكاء الاصطناعي كهاكر

## 01 التخمين

- أنظمة ذكاء اصطناعي قادرة على تخمين كلمات المرور المعقدة خلال ثوانٍ.

## 02 التصيد

تتقنيات توليد رسائل تصيد شديدة الأقناع وتحاكي أسلوب مدرائك

## 03 التقليد

- التطوير المستمر بتقنيات تقليد الصوت حتى يستعمل كنسخة صوتية رقمية عنك

## 04 الأثر الرقمي

- كل حركة على الإنترنت تترك أثرًا دائمًا، حتى بعد الحذف.

# اقتصاد الظلّ للبيانات

## 01 بورصة بيانات

- ستنشأ بورصات خفية تتاجر ببيانات الموظفين والمؤسسات كأصول مالية

## 02 بيع ملفك السلوكي

- قد يتحضر ويباع ملفك السلوكي لمن يتحدد ترقيتك او حتى قبولك في وظيفة مستقبلاً

## 03 الأنترنت العميق

- سوف تنشط الأنترنت العميق (المظلم) في عمليات البيع والشراء والتصدي

# قوانين أكثر صرامة وصراعات سيبرانية

## 01 أمن المعلومة

- النقاش الدولي المفتوح لتعظيم أهمية المعلومة

## 02 التشريعات والقوانين

- دول ستتسابق لإصدار قوانين أقوى، لكن المهاجمين سيطوّرون تقنيات تفوق هذه القوانين.

## 03 الشفافية الرقمية

- الدعوة المفتوحة لتعظيم دور الحوكمة للتصدي للعبث الرقمي

## 04 التصدي والحماية

- صراع مستمر بين من يحمي ومن يهاجم، يشبه سباق التسلح الرقمي

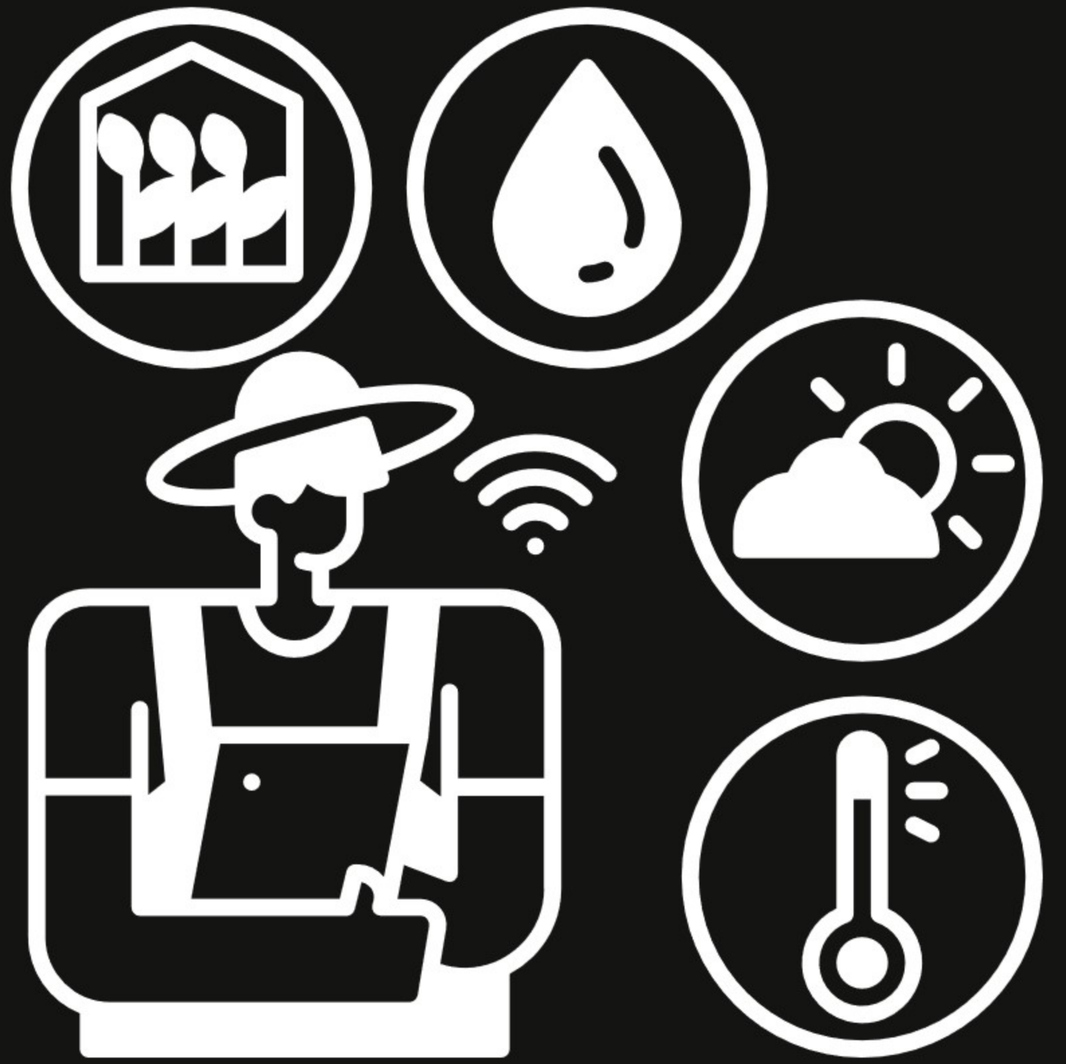
في المستقبل، لن تكون كلمة المرور وحدها كافية. سننتقل إلى الهويات اللامركزية والتوثيق البيومتري المتقدم

# ملامح عالم البيانات بعد عشر سنوات

## السلاح الأمني والأقتصادي

# بنية رقمية فائقة الترابط

- كل شيء سيكون متصلًا: المدن، السيارات، الأجهزة المنزلية، وحتى الملابس عبر إنترنت الأشياء المتقدم (IoT++).
- كل حركة أو نبضة صحية ستولد بيانات لحظية يتم تخزينها في منصات سحابية ضخمة.
- النتيجة: انفجار غير مسبوق في كمية البيانات يجعل التتبع الدقيق لأي شخص أمرًا بديهيًا.



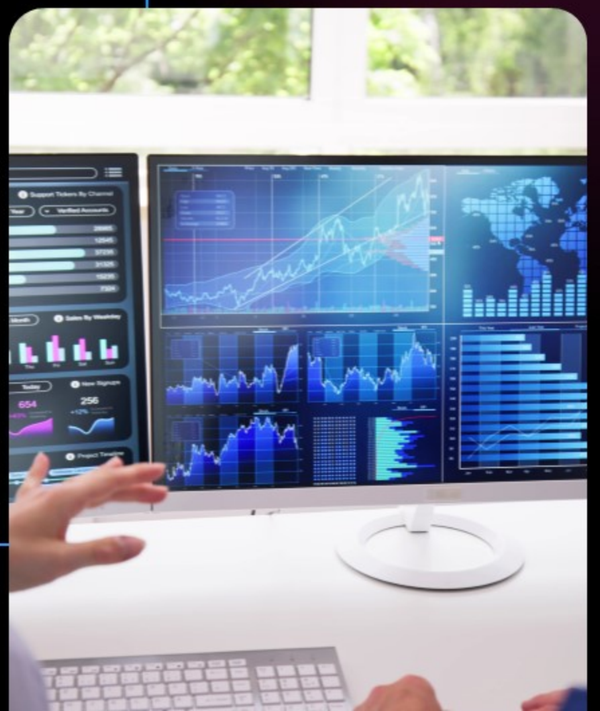
# الذكاء الاصطناعي المستقل

- أنظمة هجومية ذاتية التعلم قادرة على استهداف مؤسسات أو دول من تلقاء نفسها دون أوامر بشرية.
- خوارزميات تتنبأ بسلوك الأفراد بدقة هائلة، فتصمم رسائل تصيّد مخصصة لكل موظف.

# الحوسبة الكمّية

- أجهزة كمّية قادرة على كسر أعقد خوارزميات التشفير الحالية في ثوانٍ.
- ما نعتبره اليوم أمانًا (كلمات مرور، تشفير بنكي) سيصبح غير كافٍ تمامًا.
- سيظهر سباق عالمي لتطوير تشفير مقاوم للكمّ.

# اقتصاد بيانات أشد تعقيدًا



- ستنشأ بورصات بيانات عالمية، حيث تُباع بيانات الأفراد والمؤسسات لحظيًا لتحديد الأسعار، القروض، والقرارات الاستثمارية.
- بياناتك الصحية أو الشرائية قد تحدد تلقائيًا قيمة التأمين أو الفوائد البنكية في لحظة.

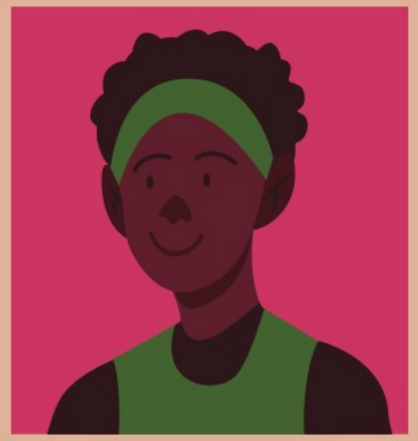
# هويات رقمية متعددة الطبقات

- سيحمل كل إنسان هوية رقمية شاملة تضم تاريخه الصحي، المالي، التعليمي وحتى سماته الجينية.
- بعض الدول قد تمنح أو تحجب خدمات أساسية (سفر، قروض، وظائف) بناءً على سمعة هذه الهوية.
- خطر الانتحال الرقمي (Deepfake Identity) سيصبح تحديًا يوميًا.

# صراع تشريعات وسياسات

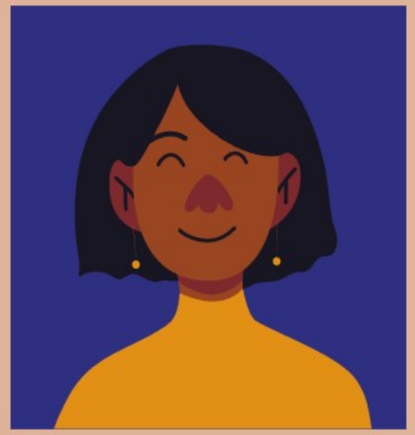
- القوانين المحلية ستكافح للحاق بالتقنيات.
- قد نرى اتفاقيات دولية لحماية البيانات مثل اتفاقيات المناخ اليوم.
- لكن المهاجمين سيبقون غالبًا أسرع من التشريعات.






# التحول الثقافي

- الوعي المجتمعي سيعتبر حماية البيانات حقًا إنسانيًا أساسيًا مثل الحق في الماء أو التعليم.
- ستصبح الخصوصية عملة ثقة تحدد علاقة المواطن بالمؤسسات والدولة.





# خط الدفاع الأول الوعي المهني أقوي من الجدار الناري

# استراتيجيات الحماية الحديثة


## Zero Trust security

## AI-driven monitoring

## Behavioral Analytics

## Cyber Hygiene Programs


# دعوة لأن نصنع أمننا بلغتنا... ولغتنا بوعينا.

"الكويت اليوم عندها قوانين لحماية البيانات، لكن الأهم من القانون... هو وعي المواطن قبل النص."

**الهدف: تعزيز فكرة السيادة الرقمية والهوية الواعية.**

"كل موظف واعٍ هو
درع بشري ضد
الحرب السيبرانية."

# Thank you