دافوس الرقمي السعودي غسيل سمعة وترويج وتطبيع

ينعقد اليوم، وعلى مدى ثلاثة أيام، مؤتمر "ليب" أو ما يُطلق عليه استعراضاً "دافوس الرقمي السعودي". النسخة الثالثة للمؤتمر ينطلق من الرياض، في استكمال لصورة غسيل السمعة التي ينتهجها النظام السعودي على عدة مستويات.

من الرياضة، إلى الفن والسجاد الأحمر، مرورا بالمشاريع العمرانية "التنموية" بما فيها من خيال وتهجير أصحاب الأرض وسرقة المال العام وإفقار الشعب، يأتي الاستثمار في الترويج والغسيل التكنولوجي بابا مستحدثا في سُلّم المشاريع والمتابعات السعودية لاعتلاء "العرش"، وسحب البساط من تحت عتبة "دبي"، لما تمثله من مركز استثماري وتجاري في الشرق الأوسط.

وعلى منوال التجمعات التي تحظى برعاية و"مباركة" محمد بن سلمان، من المتوقع انضمام ما يقرب من ألفي زائر حول العالم، بين متحدث وعارض في عالم التكنولوجيا. حيث سيشكل الحدث فرصة إضافية لتبييض السمعة وإبرام صفقات بالمليارات، غير معلوم مدى فعاليتها ضوروتها وأهميتها.

إلى جانب ما ذكر، يأتي المؤتمر في وقت تصعّد فيه مملكة الموت من سياسة التتبع والملاحقة بحق أصحاب الرأي والناشطين على مواقع التواصل الاجتماعي، وبما أننا أمام التجمع لتكنولوجي الرقمي الأكبر لخبراء العالم في البيانات والذكاء الاصطناعي في "السعودية"، ما يعني أننا أمام خطر ارتفاع مخاطر استخدام الرياض لبرامج الأمن السيبراني لغايات التجسس والتضييق على المواطنين.

هذا فضلا عن ما يمثله المؤتمر من مساحة لتعزيز التعاون الأمني، القائم أصلاً، مع الشركات التقنية الإسرائيلية. ففي حزيران/يونيو 2021، كشفت صحيفة "هآرتس" العبرية أنّ شركة "كوا دريم" تُقدم خدمات سايبر هجومية للنظام السعودي، وهي واحدة من شركات السايبر الهجومية الإسرائيلية التي تعاقد معها النظام السعودي. ونقلت الصحيفة عن مصدر قوله، إنه "بين زبائن كوا دريم أجهزة إنفاذ القانون وحكومات في عدة دول شرعية في الغرب، ولكنْ، هناك آخرون".

وتابعت الصحيفة، أن "كوا ريم" زوّدت خدماتها للحكومة السعودية منذ العام 2019، "وتكنولوجيتها معروفة لجهات أمنية تعتبر موالية لمحمد بن سلمان" وفي تموز/يوليو 2021، كشفت صحيفة "نيويورك تايمز" الأمريكية، أنّ وزارة الأمن الإسرائيلية، أصدرت تصاريح تصدير رسمية لأربع شركات تعمل في مجال البرمجة والهايتك الإسرائيلية، من بينها شركة "كوا دريم" لبيع برمجياتها الخاصة بالتجسس والقرصنة، للسلطات في السعودية. وذكرت أنه "منذ العام 2017 دخل إلى السعودية العشرات من الإسرائيليين الضالعين في الشأن الاستخباراتي، ومعظمهم من وحدات سيبرانية".

وقالت إنّ شركات السايبر الهجومي التي حصلت على تفويض للعمل مع "السعودية"، هي "إن إس أو" و"كانديرو" و"فيرينت" و"كوا دريم"، وذكرت أنّ الشركتين الأخيرتين منحتا التفويض بعد مقتل الصحفي جمال خاشقجي.

وتعتبر "إن إس أو" أكبر شركة سايبر هجومي إسرائيلية، وتبلغ قيمتها أكثر من مليار دولار، وتتخصص في ابتكار وتطوير برامج التجسس واختراق الهواتف الخلوية عبر برنامج "بيغاسوس" الذي ابتكرته وطورته. في حين أن" كانديرو" -وهي شركة منافسة ولكنها حديثة العهد- تختص بتطوير برامج التجسس واختراق الحواسيب، إذ تجيز برامجها اختراق الحواسيب اللوحية ومنظومات الحواسيب، وسرقة معلومات وبيانات والتسبب في أضرار للمضامين والأجهزة التي يتم اختراقها.

ويعد برنامج التجسس "بيغاسوس" الأكثر تقدما في العالم في الاختراق عن بعد للهواتف الخلوية وقرصنة المضامين وجمع المحتوى الموجود عليها أو الذي تم تصويره بها. كما يتيح البرنامج الإسرائيلي التجسس

على مدار 24 ساعة على مستخدم الهاتف الخلوي، عبر مراقبة الهاتف الشخصي والاطلاع أولا بأول على الرسائل والبيانات والصور والفيديوهات والمكالمات وجهات الاتصال، وأيضا تشغيل الميكروفون والكاميرا عن بعد.

هذا وتدر الصناعة الإسرائيلية للسايبر الهجومي وحدها مئات الملايين من الدولارات سنويا على الخزينة الإسرائيلية، وتعتبر شركة "إن إس أو" الرائدة في المجال والأرباح أيضا، حيث توظف 750 شخصا في "إسرائيل" وبلغاريا. وبلغ إجمالي إيرادات "إن إس أو" عام 2020 أكثر من 243 مليون دولار، إذ حققت الشركة أرباحا بلغت 99 مليون دولار، بحسب ما أفادت صحيفة "غلوبس" الإسرائيلية. وبينما تمكنت شركة "إن إس أو" خلال العام الجاري من إبرام العديد من الصفقات الضخمة التي تقدر قيمتها بعشرات الملايين من الدولارات لكل منها، وقعت الشركة المنافسة "كانديرو" اتفاقيات أكثر تواضعا".

إن مساعي "السعودية" في إعلاء مستوى مراقبتها للمواطنين، باتت تتخطى حد سَنّ القوانين وسواها من ما يمكن اعتباره كسلوك رد فعل منها على أي انتقاد داخلي. فلا يمكن النظر إلى "المدن الذكية" التي يُزعم الانتهاء من تأسيسها عام 2030، على رأسها مدينة نيوم، سوى كأداة أساسية لما يمكننا تسميته "القمع المسبق"، وهو الذي لا ينتظر تبلور السلوك بل أنه يستبقها.

يكمن هذا بما يتطلبه الانتقال إلى هذه المدن من تقديم للبيانات الشخصية، وبما تدمجه في حياة الأفراد اليومية من أحدث التقنيات، سواء باستخدام أجهزة الاستشعار، وإنترنت الأشياء، والمراقبة البيومترية، والذكاء الاصطناعي، لهدف أسياسي هو توسيع نطاق مراقبتها.

تعتمد "المدن الذكية" في جوهرها على جمع ومعالجة البيانات الشخصية على نطاق واسع، والتي يتم تنفيذها عادة دون علم الأفراد أو موافقتهم. ويتم إضافة كل معلومة جديدة عن الشخص إلى "هويته الرقمية".