22. aprile

Computer quantistico: rivoluzione medica o scomparsa della privacy?

I progressi nel campo della fisica si ottiene negando l'ovvio e accettando l'impossibile.
Robert Anson Heinlein

Secondo te la fisica quantistica ha la risposta?
Scusa, ma a che cosa mi può servire che tempo e spazio siano esattamente la stessa cosa?
Cioè, chiedo a uno che ora è e lui mi risponde "6 Kilometri".
Ma che roba è?
Woody Allen

Se la fisica quantistica non ci spaventa, è perché non l'abbiamo capita.
Jo Nesbø

Ultimamente si iniziano a calcolare le ricadute che la tecnologia dei computer quantistici potrebbe avere in un prossimo futuro. Il computer quantistico è la prossima vera rivoluzione dell'umanità, se si riuscirà a produrlo su larga scala farà fare all'analisi dati un salto pari solo al salto dalla carta al file. Ma andiamo per ordine. Si fa confusione troppo spesso tra computer quantistico e tecnologia basata sullo studio dei quanti.

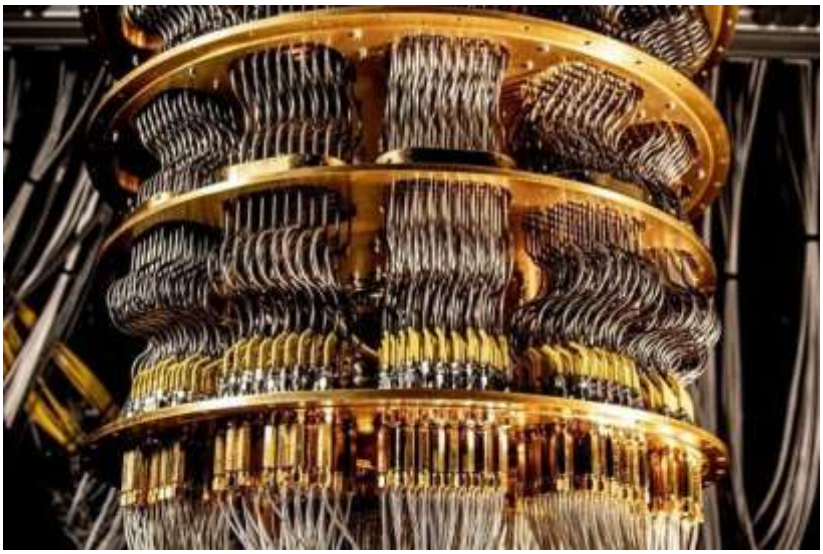
La rivoluzione dal Bit al Qubit

Il computer classico, come lo conosciamo oggi, riesce a trasmettere e riprodurre le informazione attraverso i bit. Ogni bit passa un messaggio lineare: 'positivo' o 'negativo', 0 o 1. La sequenza ordinata di bit compone informazioni. Questo è quello che chiamiamo "codice binario".

Nella tecnologia odierna è fondamentale la conoscenza della meccanica quantistica: gps e navigatori, luci led e risonanze magnetiche, sono solo alcuni esempi di tecnologie che non ne possono fare a meno per funzionare. Tuttavia la trasmissione delle informazioni rimane binaria, ancorata al bit. La differenza è che l'informazione sarà calibrata per tenere conto della meccanica quantistica.

Il computer quantistico, invece, è una rivoluzione che non abbiamo ancora nelle nostre vite: **al posto del bit utilizza il Qubit**. Immaginatevi il bit precedente come un cerchio. Il cerchio è pieno / il cerchio è vuoto. Questa è la sola informazione che può trasmettere da solo. Ora immaginate il **Qubit**, invece, come una sfera. In ogni **Qubit** possono essere sovrapposte moltissime informazioni, è come un campo tridimensionale che può essere riempito. Ogni **Qubit** può essere letto come una posizione sulla sfera, per esempio, oppure dare gradazioni di riempimento. Ogni **Qubit**, in altri termini, sopporta al suo interno messaggi molto complessi.
Per intenderci, nel 2019 Google ha adottato un computer quantistico per alcune funzioni, facendogli fare un calcolo che avrebbe necessitato di più o meno **10.000 anni di tempo a un computer tradizionale… in 3 minuti.**

Ad oggi i computer quantistici più potenti non contano più di **100 Qubit** a loro disposizione, e il vero impedimento rimane l'isolamento totale del **Qubit** (*soprattutto l'isolamento termico, che deve escludere anche i residui termici del BigBang! Quelle elegantissime strutture tubolari sono semplicemente il "frigorifero" necessario al cip*).



Le speranze in medicina dei computer quantistici

La ricostruzione a computer della struttura di una molecola è fondamentale per l'evolversi della medicina e della farmacologia.

Prendiamo a esempio una molecola d'acqua (H2O): 10.000 bit conterranno tutte le informazioni che ci servono. Piuttosto poco: le foto che scattiamo con i nostri cellulari sono ben più pesanti.
*Una molecola di Etanolo (C2H6O) necessiterà invece di 10^12 bit, e cioè di un numero di bit pari a 1 con 12 zeri a seguire. E' già parecchio, ma ci sono computer (grandi come una stanza) che possono gestire questo carico di informazioni.Quando però analizziamo la caffeina (C8H10N4O2) avremo bisogno di un numero di bit pari a 10^48. Ebbene, per analizzare compiutamente una molecola di caffeina, ad oggi, ci vorrebbe un computer grande più o meno quanto metà della luna (*non è un'iperbole, ci vorrebbe effettivamente una metratura quadrata pari*). E non siamo neanche tra le molecole più complesse*

Un *computer quantistico*, invece, è facilmente in grado di supportare anche le informazioni delle molecole più complesse, analizzarle e dare output.
In modo utopico (ma neanche troppo lontano) questo potrebbe segnare una **farmacologia completamente personalizzata e a basso costo**, studiata sui nostri parametri individuali. Sarebbe la fine dell'aspirina come la conosciamo, per accogliere una medicina che abbia solo e soltanto il nostro nome scritto sopra.

I pericoli della crittografia

I computer che usiamo oggi sono molto bravi a moltiplicare tra loro i numeri. Sanno fare immediatamente 2×3=6, e lo sanno fare a livelli di complessità impensabili per la mente umana. Il procedimento opposto, ovvero la scomposizione, consiste nel riportare ogni numero complesso a operazioni tra numeri primi. Il 6 è 'scomponibile' in 3×2.

Questo secondo procedimento, invece, è molto complicato per i computer odierni. Un numero molto alto da scomporre può impegnare un computer odierno per anni (ancora una volta non si esagera).

La ***crittografia*** si basa su questa falla del computer contemporaneo: le carte di credito, per esempio, hanno codici da scomporre che impegneranno ogni eventuale computer per più tempo della scadenza stessa della carta.
Un computer quantistico, dotato di almeno un milione di **Qubit** (oggi non esistente, ma possibile) potrebbe facilmente scomporre ogni codice che proponessimo a nostra difesa. Sarebbe la fine formale di ogni crittografia e sicurezza digitale.
Attualmente alcuni computer quantistici sono già utilizzati in modo perverso

ma il basso numero di **Qubit** a disposizione li rende quasi inoffensivi se si passa da una chiave crittografica a sicurezza AES-128 a una chiave AES-256 (se poi ulteriormente rinforzata da una VPN i nostri dati sar Computer quantistico: rivoluzione medica o scomparsa della privacy?

Come in ogni cosa, infine, non si può prevedere l'uso che si farà di questa evoluzione, e come la medicina personalizzata potrebbe aprire a scenari discriminatori terrificanti, la caduta di sicurezze digitali potrebbe portare a un uso consapevole e responsabile della rete. *Il computer quantistico non è il futuro più di quanto lo siamo noi.*

Computer quantistici resistenti agli attacchi informatici

I computer quantistici in grado di decifrare gli algoritmi di crittografia standard potrebbero arrivare tra qualche anno, qualche decennio o forse mai
Tuttavia, stanno già avendo un impatto significativo. Una nuova corsa agli *armamenti crittografici* si sta sviluppando attorno ai computer quantistici, in una dinamica che minaccia gran parte *dell'infrastruttura digitale* del mondo moderno.

I governi e le grandi aziende tecnologiche stanno cercando freneticamente modi per applicare e contrastare il potere di questa tecnologia. In particolare, stanno sviluppando schemi di crittografia resistenti agli attacchi informatici da parte di computer quantistici, noti anche come schemi di crittografia post-quantistica. La sfida: gli algoritmi quantistici resistenti possono essere vulnerabili all'hacking convenzionale.

L'estate scorsa, un computer classico che non è nemmeno in grado di eseguire Windows 11
Ha "craccato" (violato) un algoritmo di crittografia resistente ai quanti in meno di un ora.
(NIST Post-Quantum Algorithm Finalist Cracked Using a Classical PC)
Per fare un confronto, i computer classici impiegano centinaia di trilioni di anni per violare gli schemi di crittografia a chiave pubblica che sono standard in qualsiasi cosa, dalle banche ai sistemi di sicurezza.
(Breaking RSA Encryption - an Update on the State-of-the-Art)

L'algoritmo craccato, *SIKE* (Supersingular Isogeny Key Encapsulation) di Microsoft
era uno dei candidati in fase avanzata del governo degli Stati Uniti per modernizzare gli attuali standard di crittografia e impedire a potenziali avversari con computer quantistici di svelare dati altamente sensibili.
Esiste il pericolo reale che, tentando di affrontare il rischio di ***hacking quantistico***, le architetture di sicurezza possano aprire un'altra vulnerabilità più devastante e immediata. Se ***SIKE*** fosse stato schierato prematuramente su sistemi critici e la sua debolezza fosse stata scoperta da un avversario, le conseguenze economiche e di sicurezza sarebbero state terribili.

Tuttavia, continuare a fare affidamento su una crittografia convenzionale potenzialmente obsoleta può essere altrettanto pericoloso. Se i computer quantistici violassero la crittografia a chiave pubblica, ci sarebbero conseguenze significative per l'economia, la privacy e la sicurezza.

Ad esempio, gli hacker potrebbero utilizzare questa capacità per compromettere sistemi di sicurezza nazionali. Ciò esporrebbe potenzialmente informazioni classificate, inclusi dati di intelligence e militari. Inoltre, transazioni finanziarie, e-mail, firme digitali e altre informazioni riservate potrebbero essere decrittografate.

La mancanza di comprensione delle tecnologie quantistiche nei circoli politici, le tensioni internazionali e le sfide infrastrutturali complicano ulteriormente il dilemma e aumentano il rischio di errori di calcolo.

La corsa al post-quantistico.
La maggior parte delle attuali **crittografie a chiave pubblica** si basa su operazioni matematiche facili da risolvere ma difficili da annullare. Ad esempio, è facile moltiplicare due grandi numeri primi. Tuttavia, trovare questi numeri esatti fattorizzando il loro prodotto richiede molto tempo per un computer classico.
I computer quantistici potrebbero avvicinarsi alla fattorizzazione trasformandola in un problema di ottimizzazione o applicando un metodo chiamato **algoritmo di Shor** .

Quello di **Shor** è uno dei pochi algoritmi attualmente conosciuti che potrebbe consentire ai computer quantistici di funzionare notevolmente meglio dei computer convenzionali. Questa capacità migliorata potrebbe decifrare i tipi più diffusi di crittografia a chiave pubblica in modo esponenzialmente più rapido rispetto ai computer classici in modo esponenzialmente più rapido rispetto ai computer classici.

Algoritmo di Shor
Sebbene ogni numero intero abbia una scomposizione univoca in un prodotto di numeri primi, si ritiene che trovare i fattori primi sia un problema difficile. La sicurezza delle nostre transazioni

online, infatti, si basa sul presupposto che il factoring di numeri interi di mille o più cifre sia praticamente impossibile. Questa ipotesi è stata contestata nel 1995 quando Peter Shor ha proposto un algoritmo quantistico polinomiale per il problema della fattorizzazione. L'algoritmo di Shor è senza dubbio l'esempio più drammatico di come il paradigma dell'informatica quantistica abbia cambiato la nostra percezione di quali problemi dovrebbero essere considerati trattabili. In questa sezione riassumiamo brevemente alcuni fatti di base sulla fattorizzazione, evidenziamo gli ingredienti principali dell'algoritmo di Shor e illustriamo come funziona utilizzando un problema di fattorizzazione giocattolo.

I sistemi teoricamente capaci di queste imprese sono noti come computer quantistici "crittograficamente significativi" e sono probabilmente lontani decenni dall'esistenza.

Inizialmente, solo i governi potenti e le grandi aziende tecnologiche dovrebbero avere accesso a questi sistemi, a causa del loro enorme costo e complessità.
Questi computer quantistici minaccerebbero i messaggi crittografati inviati prima e dopo la loro invenzione. I paesi stanno attualmente intercettando e archiviando i dati con la la speranza di decrittografarli in seguito, se questi paesi riusciranno a sviluppare un computer quantistico capace. Questo metodo è noto come ***"raccogli i dati ora e decifrali più tardi*** "
Alcuni esperti stimano che ogni messaggio inviato oggi venga raccolto da almeno due paesi o organizzazioni private. Tuttavia, la reale portata di questa pratica è sconosciuta.

Il **National Institute of Standards and Technology** degli Stati Uniti

NIST
National Institute of
Standards and Technology

sta tentando di migliorare la crittografia a chiave pubblica stabilendo un nuovo standard crittografico post-quantistico. I nuovi algoritmi che l'istituto sta compilando non richiedono computer quantistici per il loro sviluppo. Tuttavia, la progettazione degli schemi ha richiesto molto tempo.
Dopo una competizione durata sei anni, gli organizzatori hanno selezionato quattro vincitori iniziali e selezionato altri quattro algoritmi come finalisti per una possibile futura implementazione. SIKE faceva parte di quest'ultimo gruppo.

Dopo aver annunciato i risultati, l'istituto ha incoraggiato la comunità dei crittografi a provare a decifrare i nuovi algoritmi. Questo processo di vaglio ha introdotto prospettive esterne, nel tentativo di identificare problemi che gli addetti ai lavori potrebbero aver trascurato. Solo un mese dopo l'annuncio, i crittografi dell'università di ricerca KU Leuven sono stati in grado di violare la crittografia di SIKE.

La loro ricerca ha dimostrato che un computer single-core, che applica la matematica sviluppata negli anni '90 e 2000, può decifrare l'algoritmo in circa un'ora.

Questo tipo di hack è una prova parziale che il processo di controllo sta funzionando. Se i membri del pubblico trovano vulnerabilità e le comunicano agli enti normatori, l'istituto di standardizzazione può impedire agli attori malintenzionati di sfruttare questi difetti in una fase successiva. Nel caso di ***SIKE,*** Microsoft ha incoraggiato gli hacker in generale a condividere le loro scoperte offrendo una taglia di 50.0000 dollari.

Il sistema di ricompensa ha avuto successo in questo caso. Tuttavia, non è chiaro se il denaro sarà sempre sufficiente per impedire agli hacker di provare a vendere le loro scoperte a maggiori offerenti. Potrebbero esserci altri motivi per preoccuparsi.

Jonathan Katz, professore di informatica presso l'Università del Maryland e membro della facoltà principale del Maryland Cybersecurity Center,

Ha dichiarato ad Ars Tecnica:

"Forse è un po' preoccupante che questo sia il secondo esempio negli ultimi sei mesi di uno schema che ha reso al terzo round del processo di revisione [National Institute of Standards and Technology] prima di essere completamente rotto utilizzando un algoritmo classico.
L'altro algoritmo a cui si riferisce **Katz** è ***Rainbow,*** che i ricercatori hanno decifrato all'inizio dell'anno

Katz continua a consigliare cautela, osservando che tre dei quattro vincitori del processo dell'istituto *"si basano su ipotesi relativamente nuove la cui esatta difficoltà non è ben compresa".*
Inoltre, i vetter non dispongono attualmente di un computer quantistico crittograficamente significativo da implementare contro questi nuovi schemi di crittografia. Pertanto, gli standard setter si limitano a eseguire test puramente basati sulla teoria. Fino a quando gli schemi post-quantistici non saranno sottoposti a test pratici, ci saranno domande sull'affidabilità degli algoritmi.

I pericoli della paura.
Le tecnologie quantistiche hanno acquisito un'aura di estrema complessità e occasionale urgenza. Periodicamente, una raffica di titoli sull'impatto imminente delle tecnologie quantistiche suscita responsabili politici e membri del settore che non capiscono come funziona la

tecnologia. Questa combinazione di presunta inspiegabilità e urgenza è controproducente, persino pericolosa.

Q-Day

Q-Day è una narrazione che afferma che un grande computer quantistico un giorno sarà in grado di violare improvvisamente i sistemi di crittografia a chiave pubblica esistenti. In questo scenario, il computer quantistico decritterà quasi immediatamente elementi cruciali della sicurezza e della finanza internazionale. Ne seguirebbero conseguenze catastrofiche per la difesa, insieme a perdite monetarie e un crollo della fiducia nelle architetture finanziarie e di sicurezza internazionali. È un quadro cupo.

Sebbene ***Q-Day*** identifichi alcuni rischi potenziali reali, alcune delle sue ipotesi sono contestabili. Il principale tra questi è considerare l'avvento di computer quantistici crittograficamente significativi come una questione di *"quando"* e non "se".

Esperti e istituzioni hanno sostenuto che non vi è alcuna garanzia che i computer quantistici crittograficamente significativi diventeranno mai una realtà.

Inoltre, lo scenario apocalittico di Q-Day presuppone che i computer quantistici si svilupperanno in modo esplosivo, quasi da un giorno all'altro. Considerando le numerose sfide tecniche significative che rimangono, è improbabile che i computer quantistici migliorino a questo ritmo, sebbene sia difficile prevedere quando o se si verificheranno scoperte.

Infine, la narrativa del ***Q-Day*** considera banali alcuni ostacoli importanti per condurre l'hacking quantistico. Ad esempio, ignora che gli hacker decisi a decrittografare i dati richiederebbero l'accesso a a file crittografati e tempo su un computer quantistico, che sarebbe una preziosa risorsa limitata.

Se non verificate, queste ipotesi potrebbero indurre i responsabili politici ad affrettare i processi di definizione degli standard, producendo vulnerabilità negli schemi di crittografia. I responsabili politici possono impedirlo rifiutando di vedere la tecnologia quantistica come un dominio impenetrabile e facendo invece uno sforzo per comprenderla meglio.

Le risorse gratuite pubblicate da nazioni, aziende e divulgatori scientifici possono aiutare i "curiosi quantistici" a conoscere questa nuova tecnologia .

La concorrenza internazionale sta anche esercitando pressioni su Stati Uniti, Unione eEuropea e Cina e altre nazioni affinché sviluppino **una crittografia resistente ai quanti**.

Ogni tanto, uno di questi concorrenti afferma di essere sul punto di violare la crittografia a chiave pubblica. L'ultimo episodio ha visto un gruppo di ricercatori cinesi affermare di aver progettato un nuovo algoritmo di decrittazione quantistica. Questo metodo funzionerebbe presumibilmente su computer quantistici significativamente più piccoli di quanto inizialmente ritenuto necessario per un'efficiente crittoanalisi. Tuttavia, come spesso accade in questo campo, i risultati non sono stati così signficativi come si pensava inizialmente.

Data la natura altamente sensibile delle tecnologie utilizzate per la crittografia quantistica, è molto difficile valutare i veri progressi compiuti. Le tensioni internazionali e le informazioni imperfette fanno inasprire i timori di una sorpresa strategica.
Una sorpresa strategica è un cambiamento inaspettato che sfida gli attuali presupposti strategici. In questo caso, lo sviluppo sarebbe la perdita da parte delle società di un canale di

comunicazione essenziale e sicuro. Un governo potrebbe sviluppare e utilizzare un computer quantistico crittograficamente significativo all'insaputa degli altri, lasciando i concorrenti a indovinare se sono stati violati o meno.

C'è ancora molta strada da fare prima che le società possano raggiungere un affidabile sistema di crittografia a chiave pubblica post-quantistica. Tuttavia, le aziende e i governi possono attualmente implementare misure di sicurezza per proteggere meglio i i dati e supportare la transizione alla crittografia resistente ai quanti. Queste misure vanno da quelle meno tecniche, come le valutazioni del rischio, a quelle molto complesse, come l'implementazione della distribuzione quantistica delle chiavi. I gestori di dati possono anche creare ***honeypot*** (dati crittografati ma inutili) per fuorviare gli aggressori e compartimentare i loro dati e crittografare ogni parte separatamente.

Al di là di queste soluzioni tecniche, i governi e l'industria possono istruirsi per evitare di cadere preda dell'entusiasmo. I governi potrebbero in parte allentare le tensioni internazionali mantenendo, o almeno non impedendo, dialoghi tra scienziati, ingegneri e responsabili politici per comunicare e comprendere meglio le percezioni delle minacce. Queste discussioni potrebbero aiutare a evitare scontri indesiderati.

Inoltre, discutere di hacking quantistico nelle dottrine politiche e militari potrebbe aiutare a chiarirne l'uso. Tuttavia, sarebbe difficile per gli estranei verificare se i paesi stanno seguendo dottrine o accordi internazionali che potrebbero limitare l'uso dei computer quantistici.
Idealmente, i governi e l'industria dovrebbero mitigare i rischi tecnici e politici dell'hacking quantistico, una capacità che potrebbe non realizzarsi mai, facendo anche attenzione a non fornire a tutti coloro che dispongono di un computer moderatamente moderno gli strumenti per hackerare i segreti del governo.

La Cleveland Clinic e IBM annunciano il primo computer quantistico dedicato alla ricerca nel settore sanitario
La **Cleveland Clinic** e **IBM** hanno presentato ufficialmente la prima installazione on-site nel settore privato di un computer quantistico gestito da IBM negli Stati Uniti. L'**IBM Quantum System One** installato presso la Cleveland Clinic sarà il primo computer quantistico al mondo dedicato esclusivamente alla ricerca sanitaria con l'obiettivo di aiutare la Cleveland Clinic ad accelerare le scoperte biomediche.

A chi legge

Questo Report è un adattamento di un documento presentato alla conferenza **International Student/Young Pugwash (ISYP) Third Nuclear Age nel novembre 2022.**

Baedeker/Replay del 22 aprile 2022
Sonno pandemico : jet lang sociale
(Parte prima)

Il sonno è una delle attività fisiologiche importanti svolte da tutte le specie animali. Contrariamente alla credenza prevalente di molti, il sonno non è più considerato un periodo di inattività dalla comunità scientifica del sonno. In effetti, è associato a diverse importanti funzioni richieste per una vita sana: ringiovanimento, consolidamento della memoria, modulazione della funzione immunitaria e regolazione della secrezione ormonale.
La pandemia ha influenzato il sonno in diversi modi. Per una parte considerevole della popolazione, il sonno è peggiorato in termini di qualità, durata e tempi, ma per una piccola parte è migliorato. Il sonno è stato influenzato da diversi fattori durante la pandemia di COVID-19. I lockdown senza precedenti hanno limitato gli zeitgeber (p. es., l'attività fisica, l'esposizione alla luce del giorno, il ritmo sociale, l'esposizione allo schermo, il tempo di assunzione di cibo) che regolano il ciclo sonno-veglia. Gli studi hanno anche dimostrato che un numero considerevole di persone sperimenta angoscia associata a incertezze relative al corso del trattamento e all'esito dell'infezione da SARS-CoV-2, nonché al loro impiego. Insieme, questi problemi hanno portato a cambiamenti nella durata, nei tempi e nella qualità del sonno negli individui vulnerabili .Per altri, il blocco è stato una tregua che ha aumentato la durata del sonno e migliorato la qualità del sonno, come suggerito dalla riduzione del jet lag sociale.
Qualità del sonno: Tra gli adulti La salute del sonno comprende almeno sei parametri, vale a dire la regolarità del programma sonno-veglia, la durata del sonno, i tempi del sonno e della veglia, la soddisfazione per il sonno, l'efficienza del sonno e la prontezza diurna. Queste sono tutte misure indirette della qualità del sonno. Nei diversi sondaggi una cattiva salute del sonno è stata segnalata da un quarto alla metà dei partecipanti adulti di età compresa tra 18 e 94 anni. Esiste una "geografia" del sonno, con una salute peggiore tra i residenti dei paesi dell'America Latina e dei Caraibi rispetto ai residenti del Nord America, dell'Europa e dell'Asia centrale. Una revisione sistematica riporta che nella popolazione generale, quasi un terzo aveva segnalato disturbi del sonno. In un'analisi aggregata del sonno ottenuta attraverso diversi questionari, è stato dimostrato che i disturbi del sonno sono più elevati tra gli operatori sanitari (40%) . Simile alla popolazione generale, anche tra gli operatori sanitari è stata notata una variazione geografica dei disturbi del sonno; inferiore in Cina rispetto ad altri paesi come il Bahrain e l'Iraq. Contrariamente alla deduzione intuitiva, è difficile commentare in modo affidabile se la prevalenza sia effettivamente aumentata tra il personale sanitario durante la pandemia poiché sembrava paragonabile al tempo pre-pandemico.
Una revisione sistematica di studi trasversali ha riportato che la qualità del sonno era scarsa durante la pandemia, non solo negli operatori sanitari (indipendentemente dal loro coinvolgimento nella gestione dei pazienti COVID-19 durante la pandemia) ma anche tra gli individui non ospedalizzati (indipendentemente dallo stato di infezione da SARS-CoV-2). È interessante notare che nella maggior parte degli studi è stata segnalata una scarsa qualità del sonno nonostante si trascorresse più tempo a letto. Questa è una situazione simile all'insonnia paradossale in cui, nonostante un'adeguata durata del sonno, il sonno non è "rigenerante" forse a causa di una maggiore persistenza dell' attivazione corticale. I pazienti con infezione da SARS-CoV-2 costituiscono la maggior parte del gruppo in cui la qualità del sonno era valutata "scarsa" durante la pandemia (quasi tre quarti segnalati). Ciò è in contrasto con un'altra meta-analisi, che ha riportato che solo il 34% dei pazienti con infezione da SARS-CoV-2 aveva un sonno disturbato o di scarsa qualità. Contrariamente alle segnalazioni di scarsa o peggioramento della qualità del sonno nella maggior parte degli studi, una minoranza della popolazione (6%) ha riportato un miglioramento del sonno durante la pandemia.
Complessivamente i dati disponibili mostrano che esiste una variazione geografica tra i soggetti che segnalano una scarsa qualità del sonno sia nella popolazione generale che nei pazienti affetti da infezione da SARS-CoV-2. Questi fattori potrebbero anche enfatizzare il ruolo della genetica nella loro vulnerabilità (p. es., è stato riscontrato che i geni MEIS1 e BTBD-9 iper-espressi nel' insonnia, aumentano il rischio della "sindrome elle gambe senza riposo" e in particolare di sviluppare disturbi del sonno in associazione a fattori ambientali. Tra bambini e adolescenti La qualità del sonno scadente è stata osservata tra i bambini e gli

adolescenti non ospedalizzati provenienti da Spagna e India. Il team di Dutta ha riferito di un peggioramento del sonno in un terzo dei bambini in India. Tuttavia, la qualità del sonno non è migliorato durante la pandemia. Sembrava peggiorare nella fase iniziale del lockdown per poi rimanere stabile. E rispetto agli adulti, una percentuale maggiore di bambini (43%) ha riportato un sonno più profondo durante il blocco. Programma sonno-veglia Tra gli adulti Durante la pandemia di COVID-19 sono stati segnalati due cambiamenti importanti nel programma sonno-veglia: fase del sonno ritardata ed estensione del tempo di sonno.

In un sondaggio online (Disrupted Sleep During a Pandemic) condotto in 59 paesi, quasi il 50% al 60% della popolazione adulta ha segnalato il passaggio a un'ora di coricarsi più tardi e a un'ora di veglia più tarda. Tuttavia, le cifre variano tra gli studi e uno studio indiano in particolare ha riportato che solo un terzo dei soggetti aveva orari sonno-veglia ritardati. L'estensione del sonno ha comportato una riduzione del jet lag sociale durante i blocchi e ha mantenuto un ritmo circadiano coerente per settimane. Difficoltà nell'inizio del sonno (circa 39%) e nel mantenimento del sonno (32%) è stata segnalata dalla popolazione adulta durante la pandemia di COVID-19. Tra bambini e adolescenti Ad oggi non sono disponibili meta-analisi sul programma sonno-veglia. I risultati di diversi studi individuali, d'altra parte, sembravano contraddirsi a vicenda. Uno studio ha riportato un cambiamento nelle abitudini dell' andare a dormire e svegliarsi più tardi nei giorni feriali, ma non nei fine settimana (che erano già in ritardo anche prima del blocco). Il tempo di coricarsi ritardato e il tempo di veglia ritardato sono stati segnalati tra i bambini di età compresa tra 3 e 16 anni. Ciò potrebbe essere correlato al prolungamento della latenza dell'inizio del sonno, sia nei giorni feriali che nei fine settimana. Allo stesso modo, anche la frequenza dei sonnellini è aumentata dopo il blocco in uno studio, mentre è diminuita in un altro.

Durata del sonno Tra gli adulti In media, durante la pandemia è stata segnalata una durata totale del sonno di 7 ore tra gli adulti. Coloro che dormivano per meno di 6-8 ore prima della pandemia avevano una durata del sonno ridotta durante la pandemia, mentre coloro che dormivano di solito per 6-8 ore durante il periodo pre-pandemico, non hanno segnalato alcun cambiamento nella durata del sonno o hanno avuto un aumento tempo trascorso dormendo.

Tra bambini e adolescenti Nei bambini di età compresa tra 3 e 18 anni, c'è stato un aumento del tempo di sonno totale. In uno studio, metà dei bambini dormiva 12 ore al giorno e solo un quarto dormiva meno di 8 ore al giorno. Essendo trasversale nel design, questo studio non è stato in grado di commentare il cambiamento nella durata del sonno. C'è stato un aumento del tempo di sonno totale nei giorni feriali, ma non ci sono stati cambiamenti nei fine settimana dopo il blocco. Questo varia anche geograficamente, con una variazione maggiore in Italia rispetto alla Spagna. Raggruppamenti basati sulla modifica del programma sonno-veglia Sulla base del cambiamento nel programma sonno-veglia durante la pandemia, in uno studio Di Gupta e Kumar del Department of Neurology, Division of Sleep Medicine, All India Institute of Medical Sciences identificano 3 popolazioni: tempo prolungato a letto (63% soggetti), tempo ridotto a letto (13%) e sonno ritardato (24%). (Kumar N 2022)

Un anno fa… Baedeker/Replay del 22 aprile 2021

Veicolazione attraverso la mucosa orale