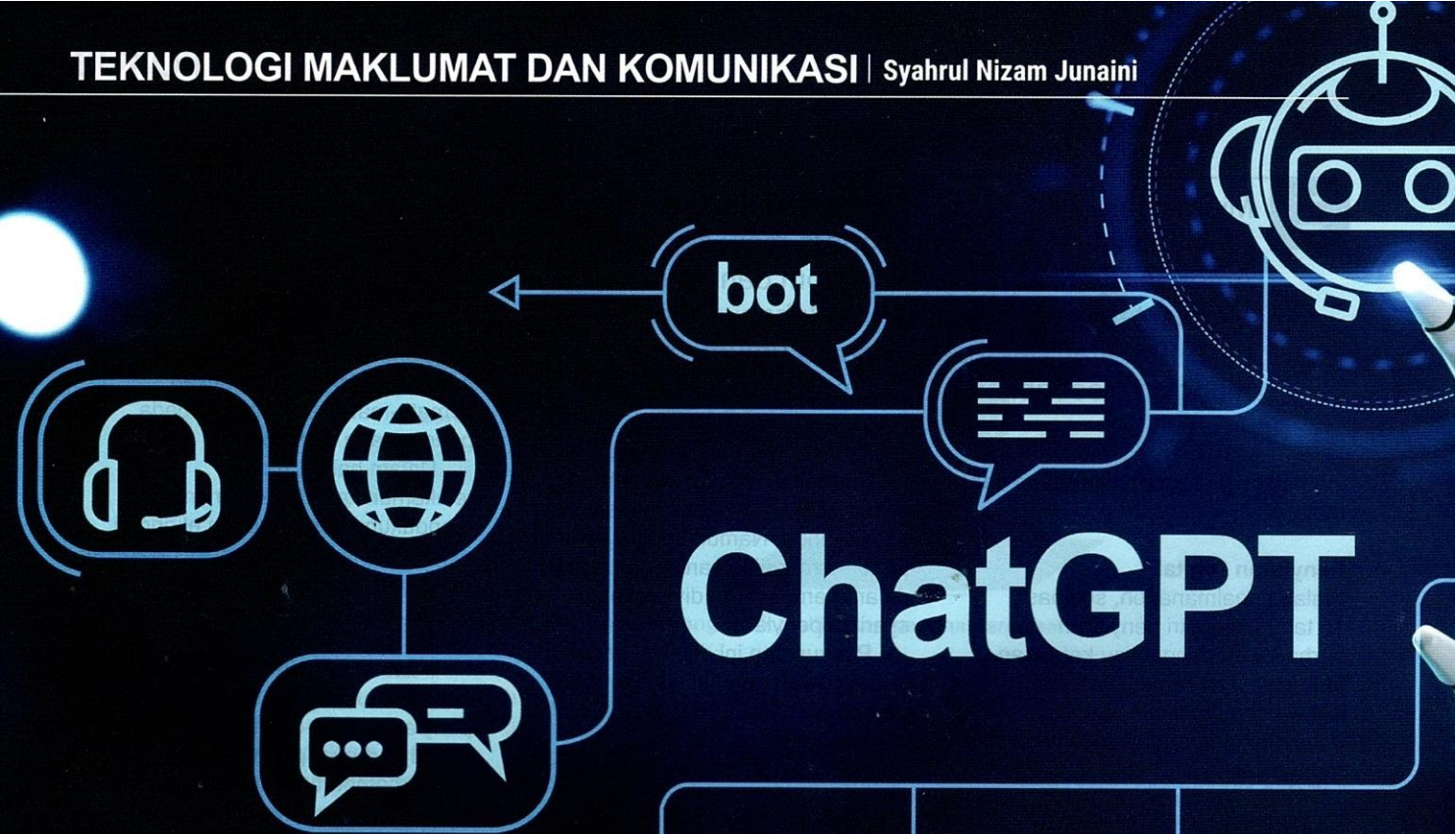


Etika, Privasi dan Sisi Gelap

ChatGPT

Dunia hari ini menyaksikan ChatGPT memercik keajaiban terbaharu dalam dunia kecerdasan buatan (AI). Aplikasi bot sembang AI atau chatbot ini dilihat begitu serba boleh, terutamanya dalam penjanaan idea dan penulisan laporan. ChatGPT juga mampu menganalisis data rencam yang menjadi bukti kepelbagaian fungsinya dalam pelbagai bidang.

Walau bagaimanapun, orang ramai perlu menyedari bahawa ChatGPT juga mempunyai batasan. Teknologi ini hanyalah program yang beroperasi berdasarkan data dan bukan mewakili otak manusia sebenar.

Algoritmanya tidak mampu berfikir seperti manusia. Oleh sebab itu, dalam sesetengah keadaan, chatbot ini mungkin memberikan respons yang berkaitan dengan isu etika dan privasi.

Era ChatGPT

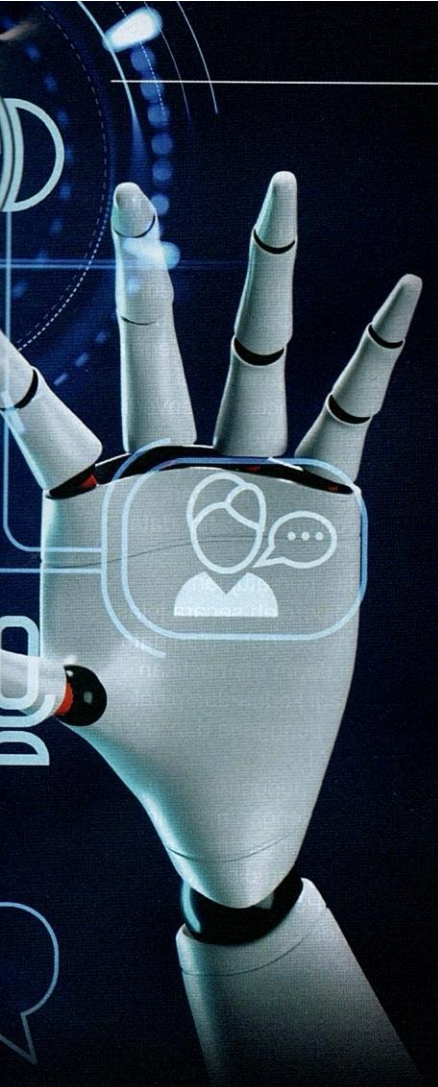
ChatGPT boleh dianggap sebagai lonjakan terkini dalam bidang AI generatif. Teknologi ini menggunakan mekanisme pembelajaran mesin bagi membolehkan manusia berinteraksi dengannya seperti berinteraksi sesama manusia.

Ethan Mollick dari Wharton University of Pennsylvania dalam artikelnya yang diterbitkan dalam Harvard Business Review pada Disember 2022 menyebut bahawa era ini sebagai "titik tolak era AI". Mengapa tidak? Dengan saiz sebanyak 175 bilion parameter (GPT-3), teknologi ini mengatasi kebanyakan model lain dalam keupayaan memahami dan mentafsirkan teks. Skala ini membuka peluang kepada analisis yang lebih kritikal dan pembangunan teks yang lebih koheren.

Sebagai perbandingan, GPT-4 memperlihat peningkatan yang ketara dalam kapasiti parameter. Menurut laporan terkini, GPT-4 terdiri daripada lapan model yang masing-masing bersaiz 220 bilion parameter. Hal ini menjadikan jumlah keseluruhan parameter untuk GPT-4 dianggarkan sekitar 1.76 trilion.

Kesensitifan Data

Isu kesensitifan data memang tidak boleh diambil ringan dalam



penggunaan ChatGPT. Pengguna harus menyedari bahawa data yang mungkin kelihatan terjamin dalam satu-satu konteks, namun boleh menjadi sensitif dalam konteks lain. Oleh sebab itu, pengguna amat digalakkan untuk berhati-hati dan mengelakkan daripada memasukkan sebarang maklumat peribadi atau berkaitan dengan organisasi.

Di samping itu, organisasi juga mesti peka terhadap berbagai-bagai situasi seperti data yang dahulunya tanpa nama (anonymous) boleh digunakan semula oleh ChatGPT untuk tujuan latihan. Hal ini bermakna bahawa terdapatnya risiko tertentu yang terlibat dalam setiap situasi tersebut. Dengan memahami konteks ini, sebarang bentuk penyalahgunaan atau kebocoran data dapat dihindari.

Dalam meluaskan huraian tentang kesensitifan data, konsep etika data harus dipertimbangkan. Dalam aplikasi seperti ChatGPT, terdapat kemungkinan bahawa data digunakan untuk analisis data berskala besar. Oleh itu, isu tatakelola, integriti dan prinsip etika dalam pengolahan data kini menjadi sangat relevan. Mengabaikan etika data juga boleh menyebabkan isu keselamatan.

Perlindungan data bukan sahaja menjadi tanggungjawab penyedia perkhidmatan, malah menjadi kewajipan kepada pengguna. Pengguna disarankan untuk memastikan bahawa mereka sendiri mematuhi garis panduan dan etika dalam memanipulasi dan berkongsikan data. Lebih-lebih lagi, bagi organisasi yang menggunakan ChatGPT dalam operasi harian, pengguna wajib memastikan protokol keselamatan data dipatuhi.

Oleh itu, pendekatan yang berhemah dan teliti perlu diambil oleh kedua-dua pihak, yakni pengguna dan organisasi dalam menggunakan ChatGPT. Hal ini bukan sahaja untuk menjamin penggunaan yang selamat dan bermoral, malah untuk memastikan integriti dan kelestarian teknologi ini pada masa hadapan.

Info Menarik

Pada 31 Mac 2023, entiti pengawasan data Itali memerintahkan OpenAI menghentikan penggunaan maklumat peribadi jutaan warga Itali yang digunakan dalam set data latihan ChatGPT.

Penggunaan dengan Berhemah

Secara umumnya, ChatGPT merupakan alat yang berguna dalam aspek interaksi dengan teknologi, namun aplikasi ini perlu digunakan dengan berhati-hati di samping mempertimbangkan batasan yang ada.

Dalam dunia yang semakin canggih dari segi teknologi, ChatGPT menjadi langkah ke arah masa hadapan yang lebih cerdas. Memang benar bahawa ChatGPT mempunyai potensi yang sangat besar untuk meningkatkan kehidupan dan produktiviti manusia, namun kedudukan aplikasi ini mesti disertakan dengan kewaspadaan terhadap isu keselamatan.

Untuk mengurangkan risiko, pengguna harus mengikut amalan yang terbaik. Hal ini termasuklah mengelakkan perkongsian maklumat yang sensitif, membaca dasar privasi OpenAI dan menolak pengumpulan data jika keadaan membenarkan.

Pengguna juga disarankan untuk menggunakan ChatGPT hanya melalui platform rasmi dan berhati-hati terhadap sambungan pihak ketiga yang mengaku dapat berintegrasi dengan ChatGPT. Kesedaran dan penggunaan ChatGPT yang bijak merupakan kunci kepada pemanfaatan teknologi ini sambil meminimumkan risikonya.

Sumber Perolehan Data

Sumber perolehan data bagi platform ini sebenarnya sukar diterangkan (walaupun oleh ChatGPT sendiri). Walau bagaimanapun, daripada sumber sekunder lain, ChatGPT menjadi titik permulaan kepada pencarian maklumat.

Dalam hal ini, ChatGPT dilihat mencari maklumat daripada Internet, namun bagaimanakah GPT boleh dianggap sebagai sumber maklumat? Oleh sebab itu, isu penting di sini ialah pengguna disarankan untuk tidak menggunakan chatbot sebagai sumber utama pencarian maklumat.

Secara umumnya, ChatGPT cukup mahir dalam menyusun perkataan. Hal ini menjadikan model ini dipanggil sebagai model bahasa

berskala besar (LLM). Keupayaan ini diperoleh daripada proses latihan data berdasarkan set data yang cukup besar.

Pada hakikatnya, ChatGPT sendiri tidak mengetahui apa-apa. Model ini hanya memilih perkataan yang paling sesuai berdasarkan data yang telah dilatih dan kemudian "memuntahkan" semula teks tersebut di paparan skrin pengguna.

Di samping itu, ChatGPT juga cenderung menghasilkan jawapan yang tidak benar tetapi disampaikan dengan penuh yakin. Hal ini dikenali sebagai halusinasi yang merujuk cubaan untuk menghasilkan fakta yang tidak benar dengan cara yang benar. Oleh sebab itu, sumber maklumat daripada ChatGPT memerlukan penapisan dan penentusahan semula.

Sebagai contohnya, pelajar universiti yang meminta ChatGPT menulis sorotan kajian akan dihidangkan dengan senarai rujukan yang tampak hebat dan mirip dengan sumber rujukan sebenar. Namun demikian, ada antara artikel tersebut sebenarnya tidak wujud. Jika wujud sekalipun, penulisnya merupakan individu yang berbeza.

Implikasi etika seperti inilah yang ketara dalam konteks sosial dan politik. Penggunaan model berkecerdasan buatan untuk menjana kandungan teks secara automatik boleh menimbulkan persoalan etika.

Dalam hal ini, terdapat keperluan untuk mempertimbangkan tanggungjawab antara editorial dengan etika media. Jika mesin (baca = algoritma) dapat menjana berita atau artikel tanpa pelibatan wartawan, siapakah yang bertanggungjawab jika maklumat yang dikeluarkan adalah salah dan menyesatkan? Hal ini juga membuka peluang kepada penyebaran berita palsu.

Oleh hal yang demikian, pengguna perlu memahami batasan teknologi ini. Meskipun ChatGPT dilatih dengan set data yang besar, namun teknologi ini tidak dapat memahami konteks atau nuansa sebenar. Teknologi ini bukan manusia dan sama sekali tidak akan memberikan jawapan yang sama seperti manusia. Hal ini juga bermakna bahawa ChatGPT mungkin tidak akan menghasilkan jawapan yang paling tepat atau benar dalam semua keadaan.

Protokol Keselamatan Data

OpenAI, iaitu organisasi di sebalik ChatGPT telah melaksanakan beberapa protokol keselamatan. Namun demikian, teknologi ini tidak bersifat selamat secara keseluruhannya.

Data pengguna (yang mungkin mengandungi maklumat peribadi) boleh sahaja terdedah jika pelayan OpenAI mengalami kompromi. Perkhidmatan yang selamat ini juga menghadapi risiko penggodaman. Hal ini boleh mengakibatkan pelanggaran hak privasi data. Lebih merisaukan jika data sensitif peribadi pengguna terdedah sewenang-wenangnya.

Selain kebimbangan privasi, respons yang dihasilkan oleh model bahasa ini mungkin tidak selalu boleh dipercayai. Oleh sebab pelbagai jenis data digunakan semasa latihan, ChatGPT kadang-kadang boleh menghasilkan kandungan yang berat sebelah, mengelirukan atau tidak tepat. Oleh sebab itu, pengguna yang bergantung pada alat ini untuk menulis artikel harus memeriksa semula hasil penulisan melalui sumber lain yang boleh dipercayai.

Penggunaan yang berniat jahat terhadap ChatGPT merupakan antara perkara yang perlu diberikan perhatian. Kemampuannya yang canggih boleh dieksploitasi untuk mencipta perisian hasad, memancing data penipuan dan berita palsu. Penjenayah siber boleh menggunakan alat ini untuk menghasilkan kandungan berbahaya dan menjadikannya sebagai alat yang berpotensi digunakan dalam aktiviti jenayah siber.

Persetujuan Pengguna dalam Konteks Privasi Data

Persetujuan pengguna menjadi asas penting dalam perbincangan mengenai privasi data dalam konteks sistem AI. Kejelasan dan pemahaman sepenuhnya mengenai tujuan dan sifat pengumpulan data adalah kritikal.

Oleh hal yang demikian, penyedia perkhidmatan seperti OpenAI perlu menyediakan dasar yang telus. Segala perkara berkaitan dengan privasi pengguna perlu diperincikan. Penyedia perkhidmatan perlu menjelaskan keperluan data pengguna dikumpulkan. Bagaimanakah pula data itu akan digunakan nanti dalam "melatih" data baharu?

Oleh sebab itu, persetujuan pengguna perlu diperoleh secara jelas sebelum sebarang pengumpulan data dilakukan. Hal ini dapat memastikan keadilan wujud bagi kedua-dua pihak, sama ada kepada pengguna dan penyedia aplikasi AI.

Sudah tentunya pengguna turut bertanggungjawab dengan memainkan peranan yang aktif dengan menguruskan maklumat peribadi yang diberikan kepada ChatGPT. Pendekatan ini mustahak bagi membina kepercayaan antara pengguna dengan penyedia platform. Keadaan ini juga sekali gus mencipta ekosistem data pintar yang lebih berasas dan beretika.

Persetujuan pengguna merupakan proses yang dinamik dan berterusan. Pengguna juga seharusnya diberikan kebenaran untuk membatalkan atau mengubah persetujuan langganan bagi tujuan pengumpulan data pada bila-bila masa.

Oleh itu, platform ini perlu menyediakan tetapan yang mudah diakses. Menu pilihan yang dipaparkan dalam platform ini perlu jelas atau tidak tersembunyi di bawah menu lain. Hal ini akan membolehkan pengguna mengawal cara data digunakan dan dikongsikan oleh OpenAI.

Pengguna perlu bebas menyesuaikan tetapan privasi mengikut perubahan keadaan atau keperluan langganan. Pengguna juga wajar memahami perubahan terhadap potensi risiko penyalahgunaan data.

Oleh hal yang demikian, konsep "keizinan bersyarat" harus diterapkan dalam platform penyedia perkhidmatan

Jangan Kongsi Data Ini

Maklumat perbankan dan kewangan

Kebimbangan terhadap eksploitasi ChatGPT oleh penjenayah siber untuk memperoleh keuntungan kewangan tidak boleh diambil ringan. Apabila pengguna memaklumkan kepada ChatGPT tentang perkara berkaitan dengan data perbankan, data itu berpotensi disalahgunakan. Hal ini termasuklah kemungkinan akses tanpa kebenaran kepada data kewangan sebenar.

Walaupun data perbankan tidak semudah itu "dicuri" oleh ChatGPT, namun risiko akses oleh pihak ketiga tetap wujud. Hal ini boleh membuka peluang untuk aktiviti berunsur jenayah seperti serangan perisian tebusan.

Maklumat kesihatan peribadi

Berkemungkinan ada dalam kalangan pengguna yang pernah meminta ChatGPT untuk melakukan diagnosis penyakit. Dalam konteks kesihatan, batasan kemampuan ChatGPT perlu difahami dengan lebih baik.

Diagnosis yang dikeluarkan oleh ChatGPT bersifat agak umum dan kurang berkemampuan dalam mempreskripsikan ubat yang tepat. Situasi ini pastinya menimbulkan kebimbangan berkenaan keselamatan penggunaan sebarang ubat-ubatan. Dalam hal ini, risiko kesihatan pengguna tidak boleh diabaikan.

Maklumat organisasi

Pelbagai data berkaitan dengan organisasi berhadapan dengan risiko terdedah kepada ketirisan data jika dimuat naik ke dalam ChatGPT.

Misalnya, insiden yang melibatkan Samsung Electronics Co. menunjukkan bahawa penggunaan chatbot bagi tujuan kerja berhadapan dengan risiko yang ketara. Syarikat tersebut juga telah melarang penggunaan ChatGPT dalam kalangan pekerja.

Keputusan ini mencerminkan kerisauan majikan terhadap risiko penyalahgunaan teknologi AI dalam ruang lingkup pekerjaan. Insiden ini berlaku apabila pekerja Samsung memuat naik kod sensitif ke dalam platform chatbot popular itu.

Maklumat keluarga

Pengguna yang berkongsikan maklumat peribadi berkaitan dengan keluarga juga menyebabkan risiko keselamatan data. Misalnya, pengguna yang menggunakan ChatGPT untuk mendapatkan maklumat tentang lokasi sekolah atau tempat tinggal orang tuanya.

Walaupun ChatGPT sendiri mungkin tidak akan "mencuri" maklumat ini, namun risiko bahawa pihak ketiga boleh mengakses maklumat yang sama tetap wujud. Hal ini juga membuka peluang kepada peningkatan risiko jenayah lain seperti penculikan atau penipuan.

AI. Hal ini membolehkan pengguna menentukan jenis data yang selesa untuk dikongsikan.

Hal ini juga bermakna bahawa walaupun pengguna hanya sekadar pelanggan, namun kuasa veto tidak terletak pada penyedia perkhidmatan semata-mata. Pendekatan ini dapat mengurangkan kemungkinan perkongsian maklumat sensitif pengguna yang mungkin tidak disengajakan.

Kekal Tanpa Nama

Tidak menggunakan nama dalam isu berkaitan dengan privasi data merupakan pilihan popular pengguna pada masa ini. Teknik ini melibatkan proses mengubah atau menghilangkan maklumat yang boleh dikenal pasti secara peribadi daripada data.

Teknik ini sering digunakan sebagai mekanisme pertahanan dalam isu berkaitan dengan privasi data. Tindakan ini melibatkan penghapusan atau pengubahan maklumat peribadi yang boleh digunakan untuk mengenal pasti individu seperti penggunaan nama samaran sebagai ganti nama sebenar.

Walaupun konsep tanpa nama menyediakan satu lapisan perlindungan tambahan, namun tindakan tersebut bukanlah jaminan privasi mutlak. Hal ini dikatakan demikian kerana proses ini dianggap tidak sah.

Laman seperti LinkedIn misalnya, memerlukan pengguna untuk menggunakan nama sebenar. Kadangkala, tidak menggunakan nama atau penggunaan identiti palsu mewujudkan persepsi yang negatif. Tindakan ini juga dipandang serong sebagai tindakan yang tidak profesional atau tidak sah.

Oleh sebab itu, walaupun tidak menggunakan nama mempunyai potensi dalam penawaran beberapa tingkat perlindungan, tindakan ini juga membawa kepada risiko dan batasan tersendiri. Pengguna dan organisasi perlu mempertimbangkan dengan teliti sejauh mana teknik ini digunakan dan konteks yang berkaitan. Hal ini adalah penting untuk memastikan bahawa kaedah tersebut sesuai dengan tujuan dan keperluan pengguna dalam melindungi privasi data.

Sebagai tambahan, penulis sendiri kadangkala memilih menggunakan konsep tanpa nama semasa melayari laman media sosial. Walaupun dianggap sebagai berprofil palsu, namun keselamatan data tetap menjadi tunjang dan fokus utama penulis.

Ts. Syahrul Nizam Junaini,
Fakulti Sains Komputer dan Teknologi Maklumat,
Universiti Malaysia Sarawak.