

BAB II

**PENGUNAAN DATA BIOMETRIK SEBAGAI ALAT PENINDASAN
TERHADAP KAUM MUSLIM UIGHUR OLEH PEMERINTAH
TIONGKOK**

Analisis ras, bangsa, dan kelompok etnis berdasarkan gambar wajah atau biasa dikenal sebagai *facial feature recognition* adalah topik populer yang berkembang di komunitas pengenalan wajah dan juga di dunia internasional. Dengan semakin pesatnya perkembangan globalisasi, maka pengenalan wajah atau *facial feature recognition* semakin memiliki potensi besar terhadap pengendalian perbatasan dan keamanan public (Douglas, 2020).

Wajah secara eksplisit menyediakan cara paling langsung dan tercepat untuk mengevaluasi informasi sosial kritis yang tersirat. Misalnya, wajah dapat menyampaikan berbagai macam informasi seperti ras, jenis kelamin, usia, ekspresi, dan identitas seseorang untuk mendukung proses pengambilan keputusan di berbagai tingkatan. Secara umum, istilah “ras” dan “etnis” sering digunakan seolah-olah kedua hal ini adalah serupa. Namun, kedua istilah ini sangat berkaitan dengan faktor biologis dan sosiologis masing-masing individu. Secara umum, istilah “ras” mengacu pada penampilan fisik seseorang, sementara istilah “etnis” lebih dipandang sebagai konsep budaya yang biasanya berkaitan dengan kebangsaan, ritual, atau warisan budaya. Sebagai contoh, mendeteksi orang Asia Timur dari keramaian orang Kaukasia adalah tugas pengenalan ras, sementara membedakan

secara visual seorang Jerman dan Perancis termasuk dalam kategori aktivitas etnis, dan karenanya memerlukan isyarat diskriminatif etnografis tambahan termasuk pakaian, sikap berperilaku, gaya berjalan, dialek, dan lain-lain.

Bagian pertama bab ini akan membahas tentang sejarah penggunaan data biometrik secara umum. Bagian kedua akan membahas tentang kegiatan *biometrics data collection* yang dilakukan oleh Pemerintah Tiongkok. Bagian ketiga akan membahas tentang prinsip dasar mengatur penggunaan data biometrik, baik dalam rezim internasional, hukum domestik yang berlaku di Tiongkok, dan analisis dari literatur akademik terkait *state-sponsored terrorism* dan *China's war on terror*.

2.1. Sejarah Penggunaan Data Biometrik

Istilah “biometrik” berasal dari kata Yunani “*bio*” yang memiliki arti kehidupan, dan “*metrik*” yang memiliki arti mengukur. Sistem teknologi biometrik hanya tersedia selama beberapa decade terakhir, dikarenakan kemajuan yang signifikan di bidang pemrosesan komputer. Banyak dari ide perkembangan teknologi biometrik ini yang berasal dari ratusan hingga ribuan tahun yang lalu (Maguire, 2009). Salah satu contoh tertua dan paling dasar dari suatu karakteristik yang digunakan untuk dikenali oleh manusia adalah wajah. Sejak awal peradaban, manusia telah menggunakan wajah untuk mengidentifikasi individu yang dikenal secara akrab dengan yang tidak dikenal atau asing. Dengan kata lain, keberagaman fitur wajah yang dimiliki oleh tiap manusia telah secara tidak sadar membuatnya sebagai bagian dari data biometrik.

Seiring perkembangannya, terdapat dua pendekatan dalam *biometrics data collection*, yang pertama adalah sistem Bertillon yang digunakan untuk mengukur

berbagai dimensi tubuh. Pengukuran ini dituliskan pada kartu yang dapat diurutkan berdasarkan tinggi, panjang lengan, atau parameter lainnya. Pendekatan kedua adalah penggunaan sidik jari yang secara formal digunakan oleh departemen kepolisian. Namun, sistem biometrik sejati mulai muncul pada paruh kedua abad ke-20, bertepatan dengan kemunculan sistem komputer (Mayhew, 2012).

2.1.1. Abad ke-19 (Tahun 1870 – 1896)

Selama ribuan tahun, manusia telah menggunakan karakteristik tubuh seperti wajah, suara, gaya berjalan, dan sebagainya untuk saling mengenali. Pada pertengahan abad ke-19, tepatnya di tahun 1870, Alphonse Bertillon, kepala identifikasi kriminal departemen kepolisian di Paris, mengembangkan dan kemudian mempraktikkan gagasan mengenai penggunaan berbagai pengukuran yang ada dalam tubuh seorang individu, misalnya tinggi, panjang lengan, kaki, dan jari yang digunakan untuk mengidentifikasi penjahat, yang disebut dengan *Bertillonage*, atau *anthropometrics*. Pelaku pidana sering kali memberikan alias yang berbeda saat ditangkap, namun Bertillon mencatat bahwa meskipun mereka dapat mengubah nama mereka, tetapi mereka tidak dapat mengubah elemen tertentu dari tubuh mereka. Namun, pada praktiknya, gagasan ini dinilai kurang akurat sampai polisi menemukan fakta bahwa beberapa orang berbagi ukuran yang sama.

Pada tahun 1892, tepat ketika idenya mulai populer, gagasan itu dikalahkan oleh penemuan yang jauh lebih penting dan dinilai lebih praktis:

kekhasan sidik jari manusia. Gagasan ini dikembangkan pertama kali oleh Sir Francis Galton, di mana Galton menulis secara rinci studi tentang sidik jari yang kemudian ia mempresentasikan sistem klasifikasi baru menggunakan sidik dari sepuluh jari manusia. Segera setelah penemuan ini, banyak departemen penegakan hukum yang menganut gagasan “pemesanan” sidik jari penjahat dan menyimpannya dalam basis data untuk menentukan identitas para penjahat. Biometrik pertama kali mulai digunakan secara luas untuk penegakan hukum dan identifikasi tujuan kriminal, izin keamanan untuk karyawan dalam pekerjaan sensitive, penentuan ayah (paternity determination), forensik, identifikasi positif narapidana dan tahanan, dan sebagainya.

Selain itu, pada tahun 1896, di akhir abad ke-19, Sir Edward Henry, seorang Inspektur Jenderal Kepolisian Bengal di India, melakukan studi dengan mencari metode identifikasi untuk diterapkan secara bersamaan atau untuk menggantikan antropometri. Henry melakukan konsultasi dengan Sir Francis Galton mengenai sidik jari sebagai metode untuk mengidentifikasi penjahat. Setelah sistem sidik jari diterapkan, salah satu pekerja Henry, Azizul Haque, mengembangkan metode pengklasifikasian dan penyimpanan informasi sehingga pencarian dapat dilakukan dengan efektif dan efisien. Sir Henry kemudian membuat sistem sidik jari Inggris pertama di London, dan sistem ini dikenal dengan *The Henry Classification System* atau Sistem Klasifikasi Henry. Sistem ini kemudian digunakan bertahun-

tahun oleh Biro Investigasi Federal (FBI) dan organisasi peradilan pidana lainnya yang melakukan pencarian sidik jari.

2.1.2 Abad ke-20 (Tahun 1903 – 1999)

Awal abad ke-20 merupakan tahun runtuhnya gagasan Bertillon, di mana hal ini didukung oleh dua pria yang ditentukan sebagai kembar identik, dijatuhi hukuman ke penjara Amerika Serikat di Leavenworth, Washington, dan ditemukan bahwa mereka memiliki ukuran yang hampir sama ketika digunakan sistem Bertillon, sehingga sistem ini dinyatakan tidak cukup untuk membedakan kedua individu tersebut.

Pada tahun 1960, sistem pengenalan wajah atau *facial recognition* menjadi semi-otomatis, dan pertama kali dikembangkan oleh Woodrow W. Bledsoe di bawah kontrak dengan Pemerintah Amerika Serikat. Sistem ini mengharuskan administrator untuk menemukan fitur seperti mata, telinga, hidung, dan mulut pada foto. Hingga pada tahun 1970, fitur warna rambut dan ketebalan bibir menjadi tambahan dalam sistem ini.

Pada tahun 1994, Dr. John Daugman dianugerahi paten untuk algoritme pengenalan iris yang kemudian dimiliki oleh IriScan, Inc. Paten ini telah dikembangkan sejak sepuluh tahun sebelumnya, yang kemudian menjadi landasan dari sebagian besar produk pengenalan iris komersial hingga saat ini. Di tahun yang sama, biometrik mulai diimplementasikan dalam pengenalan bagi para pelancong di bandara tertentu di Amerika Serikat. Istilah ini dikenal dengan Sistem Layanan Akselerasi Penumpang

Layanan Imigrasi dan Naturalisasi atau *The Immigration and Naturalization Service Passenger Accelerated Service System (INSPASS)*. Sistem layanan ini memungkinkan para pelancong untuk melewati jalur imigrasi di bandara tertentu di Amerika Serikat. Para pelancong yang berwenang menerima kartu yang telah berisi kode geometri tangan mereka. Mereka tinggal menunjukkan kartu tersebut ke perangkat biometrik. Setelah verifikasi identitas selesai, individu tersebut dapat melanjutkan ke gerbang bea cukai, sehingga melewati jalur pemeriksaan yang panjang dan mempercepat masuk ke Amerika Serikat.

Dan pada tahun 1998, FBI meluncurkan Sistem Indeks DNA Gabungan atau *Combined DNA Index System (CODIS)* untuk menyimpan, mencari, dan mengambil penanda DNA secara digital untuk tujuan penegakan hukum forensik. Sistem ini memadukan ilmu forensik dan teknologi komputer khususnya biometrik menjadi alat untuk menghubungkan kejahatan dengan kekerasan. Penggunaan sistem ini juga dipakai untuk mengidentifikasi individu yang hilang dan tidak teridentifikasi (Federal Bureau Investigation, 2015).

2.1.3 Abad ke-21 (Tahun 2000 – sekarang)

Pada abad ke-21, teknologi biometrik mengalami perkembangan yang signifikan. Dimulai pada tahun 2003, Uni Eropa mendirikan Forum Biometrik Uni Eropa atau *EU Biometrics Forum (EBF)*. Forum ini merupakan organisasi independen Eropa yang didukung oleh Komisi Eropa

(*European Commission*) yang memiliki visi untuk menetapkan Uni Eropa sebagai pemimpin dunia dalam keunggulan biometrik (The Irish Times, 2003). Organisasi ini didanai oleh Komisi Eropa dan Pemerintah Irlandia. Di tahun yang sama, pemerintah Irlandia juga memberikan dukungan terhadap rencana yang dikembangkan oleh Komisi Eropa untuk memasukkan chip biometrik ke dalam paspor warga untuk meningkatkan keamanan.

Selanjutnya pada tahun 2004, Amerika Serikat memulai penerbitan visa dari DHS (*Department of Homeland Security*) dan strategi keluar masuk AS, dibawah program Teknologi Indikasi Status Pengunjung dan Imigran Amerika Serikat atau *The United States Visitor and Immigrant Status Indication Technology (US-VISIT)*. Program ini merupakan tindakan keamanan yang dimulai di luar negeri di pos penerbitan visa Departemen Luar Negeri, dan berlanjut hingga kedatangan dan keberangkatan dari Amerika Serikat. Dengan menggunakan biometrik seperti sidik jari dan foto digital, identitas pengunjung yang membutuhkan visa dicocokkan di setiap langkah guna memastikan bahwa orang yang melintasi perbatasan Amerika Serikat adalah orang yang sama dengan penerima visa. Program ini juga menunjang kebutuhan penting Amerika Serikat akan keamanan yang lebih ketat dan komitmen berkelanjutan untuk memfasilitasi perjalanan bagi jutaan pengunjung yang datang dengan tujuan berbeda, seperti bisnis, belajar, melihat keluarga, atau berkeliling negara.

Pada tahun 2008, algoritma pengukuran jari, kualitas wajah dan kualitas iris sudah dikembangkan, membuat Pemerintah Amerika Serikat mulai mengoordinasikan penggunaan database biometrik secara menyeluruh. Hal ini memudahkan pengidentifikasian individu yang diketahui atau dicurigai sebagai teroris untuk dapat masuk ke Amerika Serikat. Akibatnya, pada tahun 2010, aparat keamanan nasional Amerika Serikat menggunakan biometrik untuk identifikasi teroris. Pada tahun 2011, CIA menggunakan teknologi pengenalan wajah untuk mengidentifikasi sisa-sisa dari jenazah Osama bin Laden.

Penggunaan data biometrik semakin berkembang di banyak negara, termasuk di Tiongkok (Council on Foreign Relations, 2021). Tindakan *biometrics data collection* telah dilakukan sejak tahun 2016. Pemerintah Tiongkok melaksanakan program *Physicals for All* yang bertujuan untuk melakukan pengawasan terhadap setiap individu mulai umur 12 sampai 65 tahun di Xinjiang. Program ini dilaksanakan oleh pihak otoritas di Xinjiang dengan mengumpulkan sampel DNA, sidik jari, *iris scans*, dan golongan darah. Program ini menggunakan teknologi biometrik dan merupakan usaha pemerintah untuk melakukan kontrol serta pengawasan terhadap kaum Uighur yang dinilai sebagai kelompok separatis dan teroris (Human Rights Watch, 2017).

2.2. Kegiatan *Biometrics Data Collection* Oleh Pemerintah Tiongkok

Sejak Mei 2014, Pemerintah Tiongkok melancarkan sebuah kampanye yang disebut dengan Kampanye Keras Melawan Terorisme, atau *Strike Hard Campaign Against Violent Terrorism*. Pada awalnya, kampanye ini digunakan oleh Pemerintah Tiongkok sebagai tindakan pemberantasan kejahatan, namun sering sekali tindakan yang dilakukan menjadi sangat kasar dan agresif. Kekasaran dan agresifitas ini didorong oleh fakta bahwa polisi atau pejabat lainnya harus mencapai tingkat penahanan yang tinggi, dan hal ini berakibat pada kecenderungan untuk mengabaikan hak-hak dasar kemanusiaan serta penangkapan sewenang-wenang dan eksekusi singkat. Tindakan ini menjadi sangat sering terjadi, terutama kepada kaum Uighur di Xinjiang.

Dibawah kepemimpinan Partai Sekretaris Chen Quango yang di transfer dari Tibet ke Xinjiang pada Agustus 2016, kekerasan dan penindasan di Xinjiang mengalami peningkatan. Hal ini juga di pelopori oleh masa awal kekuasaan Presiden Xi Jinping tahun 2013. Dalam praktik kehidupan sehari-hari, Xi Jinping telah memperketat cengkeraman pemerintah terhadap berbagai sektor, salah satunya adalah sektor keagamaan, di mana ia menyatakan pengaruh asing di Tiongkok harus dibersihkan, termasuk agama muslim yang dipeluk oleh kaum Uighur di Xinjiang.

Pada praktiknya, Kampanye Keras Melawan Terorisme ini memiliki beberapa tujuan yang dinyatakan, tetapi terutama menargetkan siapa saja yang “menentang... keamanan negara, persatuan etnis, dan stabilitas sosial” (Xinjiang Daily, 2016). Akibatnya, untuk mengetahui siapa saja masyarakat yang secara

diam-diam menyimpan sentiment anti pemerintah, maka para pejabat dan polisi melakukan pemeriksaan tingkat kesetiaan pada politik kaum Muslim Turki di Xinjiang dengan membagi menjadi tiga kategori: “dapat dipercaya” atau *trustworthy*, “rata-rata” atau *average*, dan “tidak dapat dipercaya” atau *untrustworthy*. Orang-orang yang kemudian dianggap “tidak dapat dipercaya” menjadi sasaran utama dari kampanye, serta mendapatkan pengawasan dan pembatasan yang lebih ketat. Tingkat kepercayaan ini dinilai berdasarkan kategori sosialnya, seperti apakah mereka seorang pejabat negara atau tidak, bagaimana hubungan keluarga dan sosialnya, bagaimana sikap dan perilaku mereka, termasuk juga apakah mereka sudah sering melakukan kontak kepada orang di luar negeri.

Lebih lanjut, tujuan utama lainnya dari Kampanye Keras Melawan Terorisme adalah untuk meningkatkan pengawasan yang lebih ketat di seluruh wilayah Xinjiang. Pengawasan ini sudah melibatkan penggunaan teknologi, seperti kamera CCTV dan alat pengenalan wajah yang diaktifkan kamera, tersebar di banyak wilayah, seperti stasiun bus dan kereta api, titik masuk ke kota dan desa, hotel, restoran, dan pasar. Upaya untuk memantau kaum Uighur termasuk penggunaan teknologi yang modern dan mutakhir, termasuk penggunaan data biometrik.

Sejak tahun 2016, Pemerintah Tiongkok di Xinjiang telah melakukan pengumpulan sampel DNA, sidik jari, pemindaian iris mata serta golongan darah dari seluruh penduduk yang berusia 12 dan 65 tahun. Kegiatan ini secara signifikan memperluas wewenang Pemerintah Xinjiang terhadap penduduknya hingga ke arah

negatif dan mengancam hilangnya hak asasi manusia daripada penduduk Uighur di Xinjiang (Human Rights Watch, 2017).

Dalam menganalisis kegiatan *biometrics data collection* yang dilakukan oleh pemerintah Tiongkok terhadap kaum Uighur di Xinjiang, diperlukan adanya tinjauan kembali pada keadaan hak asasi manusia di Tiongkok. Partai Komunis Tiongkok (*The Chinese Communist Party*, atau CCP) telah memerintah Tiongkok sejak berdirinya Republik Rakyat Tiongkok (*People's Republic of China*) di tahun 1949. CCP mengontrol penuh birokrasi pemerintah, termasuk wewenang atas militer, polisi, dan pengadilan. Tidak hanya itu, CCP juga memegang kendali yang erat terhadap banyak aspek masyarakat dan kehidupan publik, termasuk media massa, internet, dan akademisi. Lebih lanjut, hal ini membuat hak asasi manusia, termasuk hak atas kebebasan berekspresi, berserikat, berkumpul, dan beragama menjadi sangat dibatasi. CCP kemudian memusuhi para aktivis pejuang hak asasi manusia, termasuk aktivis yang berbicara menentang korupsi hingga protes tentang kerusakan lingkungan, dengan menghukum mereka melalui pelecehan, penahanan, penyiksaan, dan pemenjaraan oleh polisi.

Di wilayah etnis minoritas seperti Xinjiang dan Tibet, aksi untuk mengkritik pemerintah sangat sering terjadi, dengan biaya sangat besar pula yang harus dibayarkan. Pihak berwenang secara teratur menghilang secara paksa untuk menahan para kritikus dan penentang pemerintah. Hal ini telah terjadi pada hukuman seumur hidup yang dijatuhkan kepada seorang ekonom Uighur, Ilham Tohti pada tahun 2014. Tohti merupakan seorang professor di *Central University for Nationalities* di Beijing, dan adalah penduduk asli Uighur. Selama bertahun-

tahun, Tohti telah banyak menulis artikel tentang topik yang berkaitan dengan pelanggaran hak asasi manusia di Xinjiang. Hingga pada tahun 2006, dia mendirikan *Uyghur Online*, sebuah situs web berbahasa Mandarin untuk penyebaran berita yang berpusat pada Uighur, dan di platform ini, dia telah banyak melakukan kritik terhadap pengucilan populasi Uighur dari pembangunan Tiongkok, dan mendorong kesadaran yang lebih besar tentang status dan perlakuan komunitas Uighur dalam masyarakat Tiongkok. Akibatnya, aksi ini membuat Tohti dinyatakan sebagai “separatis” oleh Pemerintah Tiongkok, lalu akhirnya dijatuhi hukuman penjara seumur hidup, tanpa adanya akses kepada keluarga maupun pihak kuasa hukumnya (Front Line Defenders, 2014).

Pada awal tahun 2000, Kementerian Keamanan Publik (*Ministry of Public Security*) di Tiongkok membangun database nasional yang berisikan data DNA, dikenal dengan *Forensic Science DNA Database System*. Pada tahun 2015, Pemerintah telah mengumpulkan sekitar 44 juta “entri data lain-lain”, atau dikenal dengan *miscellaneous data entries*, dimana ini mencakup data lebih dari 40 juta individu. Setelah itu, Kementerian Keamanan Publik melakukan pencarian kedua yang bernama “*Combat Trafficking DNA Database*”, menggunakan lebih dari 513.000 sampel DNA. Pihak berwajib kemudian menyatakan bahwa database DNA tersebut digunakan untuk menyelesaikan berbagai tindakan kejahatan, seperti terorisme dan perdagangan anak, serta untuk mengidentifikasi mayat dan gelandangan, meskipun kasus-kasus yang telah terdokumentasi menunjukkan bahwa pengumpulan DNA tidak terkait dengan kejahatan yang sebelumnya dinyatakan (Human Rights Watch, 2017).

Lebih lanjut, orang-orang yang DNA-nya telah diambil oleh polisi telah banyak merinci pengalaman mereka di platform media sosial, termasuk di Weibo, Zhihu, Baidu Zhidao, Tieba, dan Tianya. Dalam postingan tersebut, banyak dari mereka menggambarkan petugas datang ke rumah, sekolah, maupun tempat kerja mereka untuk mengambil sampel DNA mereka, namun tidak ada seorang pun yang mengatakan bahwa mereka menerima surat tugas atau pemberitahuan kunjungan dari petugas tersebut. Tidak hanya itu, banyak orang yang berdiskusi tentang keharusan memberikan sampel DNA ketika mereka mengajukan pembuatan dokumen ke polisi, seperti pembuatan surat izin tinggal atau kartu tanda penduduk. Dalam beberapa kasus lain, terdapat kejadian dimana pihak polisi meminta sampel DNA dari orang-orang yang mereka bawa ke kantor polisi untuk diinterogasi, dan seringkali orang-orang tersebut bukan merupakan tersangka yang secara resmi ditahan atau ditangkap karena tindakan kriminal. Hal ini tentunya merupakan pelanggaran hak asasi manusia, dengan jenis tindakan penyalahgunaan wewenang untuk mengumpulkan DNA sebagai data pribadi individu.

Rincian pengalaman di sosial media yang berisikan keluh kesah dari masyarakat ini menyatakan ketidaknyamanan mereka tentang mengapa informasi mereka dikumpulkan, apakah koleksi tersebut sah di mata hukum, dan apakah koleksi tersebut akan berdampak pada kehidupan mereka di masa depan. Akibatnya, permasalahan pengumpulan DNA ini telah mendapat perhatian dari pers. Pada Oktober 2013, terdapat satu kasus di Provinsi Shandong, dimana polisi melakukan pengumpulan DNA terhadap lebih dari 5.000 siswa laki-laki di suatu perguruan tinggi. Sama halnya dengan kasus yang lain, para siswa tersebut tidak

mengetahui mengapa informasi mereka diambil, dan banyak juga di antara mereka yang merasa tidak nyaman atas aksi pengumpulan DNA tersebut. Saat dihubungi oleh wartawan, pihak sekolah mengatakan bahwa mereka akan bekerja sama dengan permintaan polisi terkait dengan pembuatan database tentang populasi migrasi di sekolah, namun polisi hanya mengatakan bahwa aksi pengumpulan sampel DNA tersebut adalah untuk menyelesaikan sejumlah kasus pencurian di lingkungan kampus.

Faktanya, Xinjiang merupakan wilayah yang paling tepat digambarkan sebagai salah satu dari beberapa kelompok industri pengawasan massal (*mass surveillance*) di Tiongkok. Hal ini dibuktikan dengan salah satu ciri dari infrastruktur pengawasan massal Xinjiang adalah yang disebut dengan “kantor polisi yang nyaman” atau *convenience police stations*, dimana kantor polisi ini berada di setiap sudut jalan di Xinjiang dan bersama-sama membentuk jaringan kontrol dan pengawasan yang ketat di seluruh wilayah. Selain kantor polisi, ciri dari infrastruktur pengawasan massal di Xinjiang adalah “sistem jaringan” atau *grid system* yang membagi populasi menjadi unit geometris untuk kebutuhan pengawasan yang lebih ketat dan penyediaan layanan oleh pihak Pemerintah dan aparat kepolisian.

Bukan hanya pengambilan sampel DNA dengan petugas yang datang ke rumah masyarakat, tetapi Pemerintah Xinjiang juga menggunakan aplikasi bernama IJOP (*Integrated Joint Operations Platform*), yang berguna dalam mengumpulkan data dan mengidentifikasi individu. Aplikasi ini mengumpulkan informasi dari berbagai sumber atau sensor mesin, salah satunya adalah kamera CCTV, dan

beberapa diantaranya memiliki kemampuan pengenalan wajah atau inframerah untuk penggunaan di malam hari. Selain CCTV, terdapat juga “*wifi sniffer*”, yang mengumpulkan alamat pengenal unik dari komputer, *smartphone*, dan perangkat jaringan lainnya. Sistem IJOP juga menerima informasi dari pos pemeriksaan (*checkpoints*) yang tidak terhitung jumlahnya di kawasan Xinjiang, dan juga dari sistem manajemen pengunjung (*visitors’ management system*) di area komunitas yang di awasi seperti kawasan pemukiman dan sekolah. Selain itu, beberapa dari pos pemeriksaan tersebut menerima peringatan prediktif yang didorong oleh IJOP dalam waktu nyata, dengan arti bahwa IJOP dapat mengidentifikasi target dan secara langsung memberikan peringatan untuk dilakukannya pemeriksaan dan pengawasan.

Sistem dari aplikasi IJOP diketahui menghasilkan kumpulan besar informasi pribadi, serta perilaku dan pergerakan polisi di Xinjiang. Pada 2017, perusahaan milik negara yang membangun IJOP, *China Electronics Technology Group Corporation* (CETC), mendirikan laboratorium nasional data besar yang baru untuk “kesadaran, pencegahan, dan pengendalian resiko jaminan sosial” atau “*social security risk awareness, prevention, and control*” di Urumqi, bekerjasama dengan unit investigasi khusus polisi Xinjiang dan para peneliti dari Kementerian Keamanan Publik. Laboratorium nasional tersebut membagikan dana hibah untuk penelitian dan pengembangan, dan pemeriksaan yang ditemukan pada topik penelitian tersebut menunjukkan bahwa polisi di Tiongkok sedang mengembangkan kemampuan untuk “*reality mining*”, sebuah usaha untuk mengumpulkan dan menganalisis data yang berhubungan dengan perilaku sosial

manusia, dengan tujuan mengidentifikasi pola perilaku yang dapat di prediksi. Dengan kata lain, pejabat dan polisi di Xinjiang ingin mempelajari bagaimana orang berinteraksi, dengan siapa mereka berbicara, ke mana mereka pergi, dan apa yang mereka lakukan. Hal ini dianggap sebagai sebuah pendekatan yang lebih akurat dalam menganalisis subjek dan interaksi yang dijalani, dan pada akhirnya, merekayasa dan mengendalikan realitas.

Dalam praktiknya, aplikasi IJOP merupakan alat yang multifungsi. Di luar tiga fungsi utamanya: pengumpulan data, pengarsipan laporan, dan mendorong “misi investigasi” oleh polisi, aplikasi ini memiliki berbagai fungsi yang lain, termasuk:

1. Fungsi Komunikasi (*Communication Function*) : Aplikasi IJOP mengandalkan AcroPhone, sebuah sistem komunikasi terpadu yang digunakan pejabat dan pemerintah untuk berkomunikasi di seluruh platform, seperti pesan suara, email, dan panggilan telepon.
2. Fungsi Geolokasi dan Peta (*Geolocation and Map Functions*) : Aplikasi IJOP melakukan pencatatan lokasi GPS petugas polisi dan informasi identifikasi lainnya ketika mereka mengirimkan informasi ke aplikasi IJOP. Aplikasi ini menggunakan peta dari Baidu, sebuah perusahaan teknologi besar milik Tiongkok.
3. Fungsi Pencarian (*Search Function*) : Aplikasi IJOP memungkinkan pejabat untuk mencari informasi tentang orang-orang dengan menggunakan nama, nomor KTP, nomor rumah tangga yang digunakan untuk mengakses fasilitas umum, serta alamat gedung. Selain itu,

pejabat juga dapat mengakses, atas persetujuan atasan mereka, profil lengkap dari individu tertentu.

4. Fungsi Pengenalan Wajah (*Facial Recognition Function*) : Fitur ini menggunakan fungsi pengenalan wajah oleh Face++, perusahaan pengenalan wajah yang terkenal di Tiongkok. Fitur ini digunakan untuk memeriksa apakah foto pada KTP cocok dengan wajah orang tersebut atau untuk memeriksa silang gambar pada dua dokumen yang berbeda.
5. Pendeteksian Wifi (*Wifi Detecting*) : Aplikasi IJOP melakukan pengumpulan terhadap data jaringan nirkabel (*wireless connection*) dalam jangkauan sebuah perangkat. Data yang dikumpulkan mencakup SSID (service set identifier, atau nama dari sebuah jaringan Wifi), metode enkripsi, serta lokasi GPS. Fitur ini berfungsi untuk membuat peta jaringan nirkabel yang ada di wilayah tersebut, juga dikenal sebagai “*War Driving*”, sebuah aksi mencuri data dari perangkat seseorang melalui jaringan Wifi yang lemah dan tidak aman untuk tujuan pengawasan dan infiltrasi. Fitur ini juga dapat digunakan untuk memahami kepadatan penduduk, konektivitas, dan volume data yang dihasilkan dari suatu daerah tertentu.

2.3. Prinsip Umum Yang Berknaan Dengan Penggunaan Data Biometrik

Pada dasarnya, pemrosesan data biometrik mengandung beberapa resiko bagi subjek data serta mengganggu hak fundamentalnya, dalam kasus ini adalah hak asasi manusia yang dilanggar oleh negara atas penggunaan teknologi dan data

biometrik secara ekstrim. Lebih lanjut, penggunaan data biometrik tersebut telah diatur untuk penggunaan yang manusiawi oleh beberapa prinsip umum yang akan terbagi menjadi tiga, yaitu pengaturan oleh rezim internasional, hukum domestik Tiongkok, dan menurut literatur akademik.

2.3.1. Rezim Internasional

2.3.1.1. *United Nations Compendium of Recommended Practices For the Responsible Use and Sharing of Biometrics in Counter Terrorism*

Dokumen ini merupakan ringkasan rekomendasi praktik yang dikembangkan oleh Kelompok Kerja PBB untuk Manajemen Perbatasan dan Penegakan Hukum Terkait Penganggulangan Terorisme atau *The United Nations Working Group on Border Management on Law Enforcement Related to Counter-Terrorism*, dalam kaitannya dengan Institut Biometrik.

Dokumen ini memberikan negara-negara anggota gambaran umum terkait dengan teknologi biometrik, data pribadi, serta pengoperasian biometrik dalam konteks penanggulangan terorisme. Gambaran serta penjelasan ini ditujukan terutama untuk negara-negara anggota yang memiliki sedikit hingga tidak ada pengalaman dalam pengaplikasian biometrik dan yang mungkin juga menghadapi bantuan teknis dan tantangan peningkatan kapasitas saat menggunakan teknologi biometrik ini.

Pejuang teroris asing atau *foreign terrorist fighters* (FTF) dan pelancong beresiko tinggi menjadi ancaman keamanan yang cukup besar bagi komunitas internasional. Usaha mendeteksi pergerakan teroris, dalam hal ini

adalah teroris lintas batas, termasuk usaha mengembalikan dan merelokasi FTF dan keluarganya, ked an dari zona konflik merupakan tantangan besar bagi badan keamanan dan manajemen perbatasan negara. Lebih lanjut, penggunaan teknologi biometrik, sebagaimana disyaratkan oleh Dewan Keamanan PBB dalam resolusi 2396 (2017) dapat membantu Negara Anggota untuk mendeteksi dan mengidentifikasi FTF, pengungsi dan relokasi FTF, serta teroris lainnya.

Terkait dengan prinsip dasar, *The United Nations Compendium* menyajikan ringkasan terkait dengan persyaratan tata kelola dan peraturan untuk teknologi biometrik dari perspektif hukum internasional dan hukum hak asasi manusia.

2.3.1.2. Hukum Internasional dan Hukum Asasi Manusia

Dalam perspektif hukum internasional, negara memiliki kewajiban untuk melindungi mereka yang berada dalam yurisdiksinya dari serangan teroris dan membawa pelaku tindakan tersebut ke pengadilan sambil mematuhi hak asasi manusia yang berlaku. Dewan Keamanan PBB dan Majelis Umum telah menekankan bahwa negara harus memastikan setiap tindakan yang diambil untuk memerangi terorisme mematuhi seluruh kewajiban mereka di bawah hukum internasional, khususnya hukum hak asasi manusia internasional, hukum pengungsi, dan hukum humaniter. Lebih lanjut, penghormatan terhadap hak asasi manusia dan supremasi hukum

merupakan langkah yang efektif dan penting untuk upaya penanggulangan terorisme.

Pada penerapannya, ruang lingkup dari hak asasi manusia berbeda di antara negara anggota, di mana terdapat negara yang memasukkan standar HAM internasional ke dalam hukum domestik secara berbeda. Selain itu, terdapat juga negara yang telah memperkenalkan reservasi atau deklarasi pada saat ratifikasi, sehingga hal tersebut membatasi komitmen mereka pada kewajiban perjanjian.

Dalam resolusi DK PBB 2396 (2017), Dewan Keamanan meminta negara-negara anggota untuk menilai dan menyelidiki tersangka pejuang teroris asing dan anggota keluarga yang menyertainya, termasuk pasangan dan anak-anak, dan untuk mengembangkan dan menerapkan penilaian resiko yang komprehensif bagi individu-individu tersebut.

2.3.1.3. *General Data Protection Regulation (GDPR) of European Union*

Peraturan Perlindungan Data Umum atau *General Data Protection Regulation* (GDPR) merupakan peraturan yang berkaitan dengan perlindungan perorangan sehubungan dengan pemrosesan data pribadi dan aturan yang berkaitan dengan pemrosesan serta pergerakan data pribadi (Intersoft Consulting, 2016).

Pada April 2016, Parlemen Eropa mengadopsi GDPR serta menggantikan arahan perlindungan data atau *data protection directive* yang dinilai sudah ketinggalan zaman dari tahun 1995. GDPR membawa ketentuan

umum yang mewajibkan bisnis untuk melindungi data pribadi dan privasi warga negara EU dalam pelaksanaan transaksi yang terjadi di dalam negara anggota EU. Selain itu, GDPR juga mengatur ekspor data pribadi di luar EU (Nadeau, 2020).

Sehubungan dengan *biometrics data collection*, GDPR memiliki beberapa prinsip yang mengatur tentang penggunaan data biometrik dan keterkaitannya dengan hak asasi manusia, yang ditulis oleh Els J. Kindt dalam buku *Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis*.

Lebih lanjut, dalam hubungannya dengan data biometrik, terdapat prinsip Larangan Untuk Menggunakan Data Biometrik Untuk Tujuan Diskriminasi atau *Prohibition to Use Biometric Data for Racial Or Ethnic Origin Or Health Information And Confirmation of Prohibition to Discriminate*. Prinsip ini merupakan prinsip yang dapat membatasi penyalahgunaan data biometrik untuk tujuan diskriminasi, baik terhadap ras, etnis, serta penyalahgunaan informasi kesehatan untuk tujuan diskriminasi. Menurut Kindt, memasukkan data biometrik ke dalam daftar data sensitif tidak akan menyelesaikan masalah. Kegiatan *biometrics data collection* sampai saat ini merupakan kegiatan yang masih terbuka untuk interpretasi, didasari pada fakta bahwa undang-undang perlindungan data nasional untuk data sensitif masih memiliki pandangan yang berbeda (Kindt, 2013).

Pada dasarnya, masalah yang muncul adalah meskipun data pribadi yang sensitif sudah diatur oleh negara dalam undang-undang perlindungan

data nasional, masih akan terdapat penyalahgunaan untuk menyimpulkan atau mengungkap informasi terkait kesehatan serta informasi ras atau etnis individu ataupun sekelompok orang. Penggunaan seperti itu tidak dapat diterima kecuali jika hukum khusus akan menentukan dalam kondisi apa hal tersebut akan diizinkan.

Pada tahun 1997, Council of Europe mengeluarkan aturan serta rekomendasi terkait dengan perlindungan data medis yang dikenal sebagai *Council of Europe on the Protection of Medical Data*. Pada rekomendasi 4.8, dikatakan bahwa pada analisis DNA forensic tidak hanya dibutuhkan undang-undang khusus, tetapi juga dibutuhkannya tujuan terbatas dari penggunaan dan meralang untuk menentukan karakteristik lain yang mungkin terkait secara genetik dari data tersebut. Lebih lanjut, pemrosesan data genetik untuk tujuan prosedur peradilan atau investigasi kriminal harus menjadi subjek hukum khusus yang menawarkan perlindungan yang sesuai. Data tersebut hanya boleh digunakan untuk menentukan apakah ada kaitan genetic dalam rangka menambahkan bukti, untuk mencegah bahaya yang nyata atau untuk menekan tindak pidana tertentu (University of Minnesota, n.d.).

2.3.2. Hukum Domestik Tiongkok

Pengawasan masal atau *mass surveillance* telah lama di praktikan di Tiongkok. Kegiatan ini dimulai sejak tahun 1949, di mana negara dan Partai Komunis Cina (*The Chinese Communist Party, CCP*, atau “*Party*”) telah lebih dahulu mengandalkan pengumpulan informasi dan alat manajemen sosial untuk

melaksanakan kontrol ketat atas masyarakat, terdiri dari pengumpulan unit kerja “*danwei*”, sistem pendaftaran kependudukan “*hukou*”, dan file politik rahasia “*dang’an*” (Juneja, 2017). Instansi pemerintah secara teratur mengumpulkan berbagai informasi pribadi tentang individu, mulai dari pandangan politik mereka hingga informasi tentang penggunaan kontrasepsi oleh wanita, dan menghubungkannya ke nomor identitas mereka, tanpa ada individu yang memiliki kemampuan untuk menentang aksi koleksi data pribadi tersebut.

Pada dasarnya, sistem pengawasan massal ini diterapkan diseluruh wilayah di Tiongkok, tetapi Xinjiang mengambil langkah yang paling jauh dalam penerapannya. Pihak otoritas Xinjiang berpendapat bahwa penggunaan sistem yang agresif diperlukan untuk melawan tiga kekuatan jahat: separatisme, terorisme, dan ekstrimisme (Xinjiang Daily, 2019).

Dibawah *Strike Hard Campaign*, pihak otoritas Xinjiang telah mengumpulkan data biometrik, seperti sampel DNA, sidik jari, pemindaian iris mata, dan golongan darah seluruh penduduk di wilayah tersebut antara usia 12 dan 65 tahun. Selain itu, pihak otoritas juga telah mewajibkan masyarakat Xinjiang untuk memberikan sampel suara saat mereka mengajukan pembuatan paspor guna mengumpulkan lebih banyak data tentang masyarakatnya.

Hukum domestik yang dimiliki oleh Tiongkok saat ini juga tidak memenuhi standar privasi internasional dan tidak memberikan perlindungan yang berarti terhadap pengawasan pemerintah yang dianggap melanggar hukum atau menyalahgunakan data biometrik. Pasal 40 pada Konstitusi Tiongkok atau *The Chinese Constitution* menjamin “privasi korespondensi”, tetapi Tiongkok sendiri

tidak memiliki undang-undang privasi atau perlindungan data yang terpadu (Xiaopeng, 2018).

Lebih lanjut, terdapat undang-undang, peraturan, arahan, serta aturan Tiongkok yang memberdayakan berbagai entitas pemerintah untuk mengumpulkan dan menggunakan bermacam-macam data pribadi, dan beberapa diantaranya memberikan otoritas kekuasaan yang luas dalam praktik pengumpulan data. Misalnya, undang-undang di Tiongkok yang berkaitan dengan keamanan negara, seperti Undang-Undang Keamanan Negara atau *State Security Law*, menginvestasikan polisi dan agen keamanan negara lainnya dengan kewenangan luas untuk mengumpulkan intelijen yang melibatkan keamanan negara. Undang-undang seperti itulah, yang menurut UNHRC, memberikan keleluasaan tak terbatas kepada badan-badan yang melaksanakan pengawasan, serta secara bersamaan melakukan pelanggaran terhadap norma-norma hak privasi internasional (Human Rights Council, 2014).

2.3.3. Literatur Akademik: *Human Rights, State Oppression, Biometrics Data Collection*

Pada dasarnya, bagian ini merupakan sambungan dari dua diskusi yang sebelumnya dijelaskan di atas, dan akan berbicara tentang bagaimana pengawasan terhadap manusia adalah pelanggaran dari konsep hak asasi manusia, dan secara bersamaan membenarkan konsep negara sebagai penindas (*state as oppressor*).

Seperti diketahui, hak asasi manusia (*human rights*) merupakan istilah yang sangat kuat dan sering diasosiasikan dengan terbentuknya PBB di tahun 1945, dan diadopsi oleh Majelis Umum PBB tentang Deklarasi Universal Hak Asasi Manusia

(DUHAM) tahun 1948 (Griffiths, et al., 2008). Hak asasi manusia sendiri telah melekat dan dikembangkan secara internasional, dan sebagian besar negara juga telah mengadopsi konstitusi serta undang-undang lain yang secara formal melindungi hak asasi manusia, seperti deklarasi, pedoman dan prinsip yang memberikan kontribusi pada pemahaman serta implementasinya.

Lebih lanjut, hukum hak asasi manusia internasional menetapkan kewajiban yang harus dihormati oleh negara. Dengan kata lain, dengan negara menjadi pihak dalam perjanjian internasional, negara memikul kewajiban di bawah hukum internasional untuk menghormati, melindungi, serta memenuhi hak asasi manusia. Negara memiliki kewajiban untuk menghormati, yang berarti negara harusnya menahan diri untuk tidak mencampuri atau membatasi hak asasi manusia, dan berarti bahwa negara harus melindungi serta memfasilitasi rakyatnya untuk memenuhi hak asasi manusia (United Nations Human Rights Commissioner, n.d.). Namun, pada praktiknya, negara tidak selalu melindungi rakyatnya dan memenuhi hak asasi manusia yang seharusnya diberikan pada rakyatnya. Artinya, alih-alih menjadi pelindung, dalam kasus ini, negara menjadi penindas, atau *state as oppressor*.

Penindasan atau *oppression* didefinisikan oleh kamus Merriam-Webster sebagai pelaksanaan otoritas atau kekuasaan yang tidak adil atau kejam, terutama dengan pengenaan beban, kondisi terbebani, tindakan menekan, rasa berat atau halangan dalam tubuh atau pikiran. Dengan kata lain, definisi ini menunjukkan intensitas penindasan, dan bahwa penindasan merupakan tindakan sosial yang

menempatkan pembatasan berat pada individu atau kelompok tertentu (Palmer, et al., 2019).

Dalam konteks negara menjadi penindas, Tiongkok dimaksud sebagai aktor yang memberikan teror dan rasa ketakutan bagi subjek penindasannya, yaitu kaum Uighur. Aksi *biometrics data collection* serta pengawasan massal (*mass surveillance*) yang dilakukan oleh Tiongkok telah melanggar hak asasi manusia dan konsep negara sebagai pelindung. Hal ini juga dapat diartikan sebagai ketidakmampuan dan ketidakpedulian negara dalam pemenuhan kewajibannya, yaitu untuk melindungi serta memfasilitasi rakyat untuk menikmati hak asasi manusia.