Perlindungan Data Pribadi dalam Perspektif *Sadd Dzari'ah*

Mohammad Farid Fad
UIN Walisongo Semarang
e-mail: mohammadfarid@walisongo.ac.id

Abstrak

Dalam dunia komputasi dan digital, seorang individu dituntut untuk mengenali dan menetapkan garis batas atau batasan preferensinya untuk mencapai kesepakatan tentang status privasinya dalam konteks atau ruang tertentu. Dengan kata lain, masing-masing individu harus memperoleh hak untuk menggunakan data pribadinya sendiri, yang akan memastikan peran yang lebih aktif dalam pengelolaan data pribadinya. Sementara di sisi yang lain, data atau informasi pribadi telah menjadi sesuatu yang sangat berharga, sekaligus rentan sebagai komoditas hingga menimbulkan resiko kerawanan penyalahgunaan ataupun pencurian data pribadi. Untuk itu diperlukan analitis mitigasi resiko secara syar'i demi terhindar dari kejahatan pencurian dan penyalahgunaan data pribadi di ruang siber yang disebut metode sadd dzari'ah. Penelitian ini memakai pendekatan kualitatif. Metode pengumpulan data yang dipakai dalam penelitian ini adalah metode literature, dokumentasi dan observasi. Dalam menganalisis data yang telah terkumpul, peneliti akan menggunakan analisis deskriptif-analitis dengan pendekatan ushuliyah. Temuan penelitian ini adalah dalam perspektif sadd dzari'ah, data pribadi memuat kehormatan, dan martabat pribadi yang tidak boleh diganggu. Ketika terjadi penyalahgunaan data, maka menimbulkan bahaya (mudharat) berupa rusaknya harkat dan martabat seseorang (hifz al-irdh) padahal syariat Islam sebisa mungkin mewujudkan kemaslahatan bagi manusia. Oleh karena itu, Pemerintah wajib menyusun Undang-Undang Perlindungan Data Pribadi demi menciptakan ekosistem digital yang terlindungi dan terjamin keamanannya.

Kata Kunci: Perlindungan, Data Pribadi, Sadd Dzari'ah.

Abstract

In the world of computing and digital, an individual is required to recognize and define the boundaries or boundaries of his preferences in order to reach agreement on the status of his privacy in a particular context or space. In other words, each individual should acquire the right to use his/her own personal data, which will ensure a more active role in the management of his/her personal data. While on the other hand, personal data or information has become something that is very valuable, as well as vulnerable as a commodity so that it poses a risk of vulnerability to misuse or theft of personal data. For this reason, it is necessary to analyze risk mitigation in a syar'i manner in order to avoid the crime of theft and misuse of personal data in cyberspace called the sadd dzari'ah method. This research uses a qualitative approach. Data collection methods used in this study are literature, documentation and observation methods. In analyzing the data that has been collected, the researcher will use descriptive-analytical analysis with ushuliyah approach. The findings of this study are in the perspective of sadd dzari'ah, personal data contains honor and personal dignity that should not be disturbed. When there is misuse of data, it creates a danger (mudharat) in the form of damage to a person's dignity (hifz al-irdh) even though Islamic law as much as possible creates benefits for humans. Therefore, the Government is obliged to draw up a Personal Data Protection Law in order to create a protected and guaranteed digital ecosystem.

Keywords: Protection, Personal Data, Sadd Dzari'ah.

A. Pendahuluan

Revolusi digital 4.0 telah memunculkan inovasi-inovasi baru dalam memperoleh, mentransmisikan, menyimpan bahkan memanipulasi data secara *real time* dan lebih kompleks. Perubahan ini di satu sisi memicu lahirnya terobosan-terobosan teknologi dan komputasi semisal *Internet of Things*, kecerdasan buatan (*artificial intelligence*), robotika, bioteknologi dan komputasi kuantum.

Namun di sisi lain, data atau informasi telah menjadi sesuatu yang sangat berharga, sekaligus rentan sebagai komoditas. Peran penting informasi dalam ekonomi global dan implikasi dari pengumpulan, penggunaan, pemrosesan, dan

pengungkapan data pribadi telah menimbulkan kekhawatiran tentang cara masuknya dimana data pribadi harusnya dilindungi.

Problem perlindungan data pribadi semakin urgen linier dengan meningginya penggunaan internet. Seiring waktu, penggunaan data pribadi terus meningkat, mengingat penggunaan *cyber area* semakin meningkat, pada tahun 2017 yang mencapai lebih dari 4,2 miliar orang, dibandingkan tahun 2016 yang hanya mencapai 3,7 miliar pengguna internet. Berdasarkan data tersebut, pengguna internet telah mengatasi 54,4% seluruh populasi manusia yaitu sekitar 7,6 miliar orang. Bahkan pada tahun 2020, pengguna Internet di Indonesia telah mencapai 175,4 juta orang dengan penetrasi 64%, yang berarti 64% dari 272,1 juta penduduk Indonesia aktif menggunakan Internet[1].

Dampak internet dalam dunia ekonomi telah melahirkan istilah baru yang disebut "ekonomi digital" yang diperkenalkan oleh Don Tapscott pada tahun 1995[2]. Di era ekonomi digital, perlindungan data pribadi konsumen harus dimasukkan sebagai salah satu aspek perlindungan konsumen. Masalah terbesar yang dialami oleh pengguna *e-commerce* adalah klausul standar dalam kontrak perlindungan data pribadi yang harus disepakati oleh pengguna sebelum menggunakan platform *e-commerce*.

Dalam perdagangan elektronik, dimana setiap hari berbagai jenis transaksi dijalankan, data pribadi konsumen yang ada sering kali dikirimkan tanpa adanya pengawasan. Seringkali, pengusaha atau pembuat situs web melanggar dan mempublikasikan informasi tanpa izin dari pemilik data pribadi. Artinya,

---

[1] Bayu Sujadmiko, "The Urgency of Digital Right Management on Personal Data Protection," *INTERNATIONAL JOURNAL OF RESEARCH IN BUSINESS AND SOCIAL SCIENCE* 10, no. 1 (2021): 253–258.

[2] Millencia Ang, "Consumer'S Data Protection and Standard Clause in Privacy Policy in E-Commerce: A Comparative Analysis on Indonesian and Singaporean Law," *the Lawpreneurship Journal* 1, no. 1 (2021): 100–113, http://journal.prasetiyamulya.ac.id/journal/index.php/TLJ/article/view/523.

data pribadi, mungkin saja digunakan secara tidak benar, baik untuk tujuan periklanan atau untuk dikirimkan ke pihak ketiga.

Sementara dalam konsep perlindungan informasi pribadi disyaratkan bahwa hanya pemilik data yang berhak membagikan datanya ataupun menukar informasi pribadinya pada pihak lain. Untuk itulah, pemilik konten atau pembuat situs web harus menjaga kerahasiaan data pribadi, baik untuk kepentingan pelanggan mereka serta untuk menghindari konsekuensi hukum.

Tanpa disadari, data pribadi bisa bertransformasi menjadi produk yang dapat dibeli dan ditukar, berkembang menjadi aset dan komoditas yang bernilai tinggi. Hal ini mengakibatkan semakin tingginya nilai ekonomis dari data pribadi seseorang yang rawan dipergunakan secara tidak bertanggungjawab. Bahkan tak jarang informasi pribadi tersebut justru diperjualbelikan dengan tanpa sepengetahuan pemiliknya, misalnya untuk jaringan iklan atau pialang data. Hal ini tentu saja mengganggu ranah privasi sekaligus rawan menimbulkan kejahatan digital.

Fenomena ini tentu saja menimbulkan kekhawatiran tersendiri tentang monetisasi data pribadi konsumen yang terdaftar di aplikasi *e-commerce*[3]. Dari sinilah, konsumen *e-commerce* menghadapi ancaman privasi dan keamanan yang konsisten dan berkelanjutan, ketika mereka memutuskan untuk menjadikan Internet sebagai tulang punggung mereka untuk berbelanja atau aktivitas lainnya.

Padahal penyalahgunaan data pribadi biasanya digunakan untuk tujuan kriminal, penipuan, atau kepentingan politik, hal tersebut tentunya sangat merugikan pemilik data. Salah satu contohnya adalah pada tahun 2018 lalu, Facebook harus membayar denda Rp. 70 triliun akibat tersandung kasus

[3] Raphael Haganta, "Legal Protection of Personal Data As Privacy Rights Of E-Commerce Consumers Amid The Covid-19 Pandemic," *Lex Scientia Law Review* 4, no. 2 (2020), 77-90.

penyalahgunaan data pribadi, sebanyak 87 juta data pengguna berada di *Cambridge Analytica* yang diduga disalahgunakan untuk keperluan Pilpres AS tahun 2016[4].

Kasus terbaru adalah soal bocornya data kepesertaan 279 juta Badan Penyelenggara Jaminan Sosial (BPJS) Kesehatan yang diduga diretas dan diperjualbelikan dalam sebuah forum internet. Padahal datanya meliputi nomor telepon, alamat email, gaji, hingga nomor induk kependudukan[5]. Pelanggaran informasi privasi seperti ini telah menimbulkan kekhawatiran bangsa atas perlindungan hukum yang berlaku untuk data elektronik warga Indonesia.

Hal ini harusnya menjadi perhatian khusus bagi Pemerintah untuk segera membuat peraturan untuk melindungi data pribadi sehingga menjamin keamanan bagi pengguna sekaligus memberikan sanksi yang memberikan efek jera bagi pihak yang sengaja menyalahgunakan data. Tujuannya tak lain agar dapat memberikan keamanan bagi pengguna dan dapat memberikan sanksi yang memberikan efek jera bagi pihak yang dengan sengaja menyalahgunakan data tersebut. Apalagi peraturan perundangan yang ada terkait data pribadi di Indonesia belum memberikan perlindungan yang memadai terutama terkait penggunaan kecerdasan buatan sehingga kurang memadai untuk mendorong perkembangan ekosistem ekonomi digital.

Sementara dalam kerangka hukum Islam sendiri, dikenal suatu metode hukum yang bersifat protektif, yang disebut *sadd dzari'ah*. *Sadd dzari'ah* bisa disebut sebagai salah satu terobosan hukum yang bertugas mencegah jangan

---

[4] Wahyunanda Kusuma Pertiwi, "Facebook Didenda Rp 70 Triliun Akibat Skandal Cambridge Analytica," n.d., https://tekno.kompas.com/read/2019/07/14/08170087/facebook-didenda-rp-70-triliun-akibat-skandal-cambridge-analytica, diakses 17 Juni 2021 pukul 15.49 WIB.

[5] Rahmat Nur Hakim, "Polri: Diduga Keras Data Kependudukan BPJS Kesehatan Bocor," n.d., https://nasional.kompas.com/read/2021/06/04/06300041/polri--diduga-keras-data-kependudukan-bpjs-kesehatan-bocor, , diakses tanggal 9 Juni 2021 pukul 18:54 WIB.

sampai terjebak dalam potensi kemafsadatan. Metode ini bekerja dengan memblokir semua akses yang berpotensi menuju hal yang dilarang. Kemudian, bagaimanakah sadd dzari'ah memandang urgensi peraturan tentang perlindungan data pribadi? Penelitian ini akan memfokuskan diri dalam mengkaji perlindungan data pribadi dalam perspektif sadd dzari'ah.

B. Metode Penelitian

Penelitian ini menggunakan pendekatan kualitatif. Sumber data yang digunakan yakni sumber data primer dan data sekunder. Adapun data primer yang digunakan pada penelitian ini adalah dokumentasi dan observasi. Data sekunder pada penelitian ini didapatkan dari data yang didapatkan dari kitab, artikel jurnal ataupun buku yang terkait dengan perlindungan data pribadi dan sadd dzari'ah. Penelitian ini merupakan penelitian berbasis kualitatif dengan menggunakan analisis deskriptif analitik. Metode pengumpulan data yang digunakan dalam penelitian ini adalah metode literatur, dalam menganalisis data yang telah terkumpul, peneliti menggunakan analisis deskriptif-analitis dengan pendekatan ushuliyah, artinya adalah menggambarkan atau menguraikan hasil dari pengamatan (observasi atau gejala, dan kondisi aktual) dengan cara menyelaraskan konsep perlindungan data pribadi dalam perspektif sadd dzari'ah.

C. Hasil dan Pembahasan

Seiring dengan pesatnya pertumbuhan ekosistem digital dan pasar elektronik, data pribadi telah mengambil peran kunci bagi semua individu yang secara aktif terlibat dalam proses tersebut. Seringkali ketika seseorang ingin melakukan transaksi atau pendaftaran di suatu organisasi atau *mailing list* di internet, pengguna harus mengirimkan data pribadinya terlebih dahulu dan data ini dicatat/disimpan dalam sistem elektronik.

Segala jenis transaksi, mulai dari pembayaran produk atau layanan hingga pendaftaran di situs web, memerlukan penggunaan informasi dan data pribadi secara ekstensif. Sering terjadi pengguna internet kemudian menerima berbagai pesan iklan (*junk mail*) di *inbox* mereka, yang kemungkinan besar berasal dari kebocoran data pribadi yang telah diberikannya[6].

Sementara di sisi yang lain, peningkatan minat akan informasi pribadi menimbulkan resiko kerawanan penyalahgunaan ataupun pencurian data pribadi. Apalagi di tengah pandemi Covid-19 yang membuat seseorang tanpa sadar sering meninggalkan jejak data pribadinya di dunia maya. Akibat tak adanya pengawasan hukum, seringkali pemilik website melanggar dan mempublikasikan informasi tanpa meminta izin dari pemilik data. Artinya, data pribadi, mungkin digunakan secara tidak semestinya, baik untuk tujuan periklanan maupun untuk mengirimkannya ke pihak ketiga. Hal ini terjadi karena trafik pengiriman data dan informasi yang semakin global, dan konsep *open system authentication* yang terdapat dalam jaringan hingga memudahkan seseorang untuk masuk ataupun menyusup secara illegal ke dalam jaringan lain.

Dunia siber seolah memberikan "kesempatan" kepada setiap pihak sebagai calon korban atau pelaku kejahatan baik disadari maupun tidak. Sebagai contoh, di media sosial, fitur media sosial memungkinkan orang untuk membagikan data pribadinya tentang diri mereka sendiri seperti foto, video, alamat, tempat yang mereka kunjungi, dan informasi intim lainnya, menyalahgunakan manfaat internet yang biasanya digunakan untuk melecehkan ataupun bernada mengancam. Akhirnya, itu menciptakan bentuk kejahatan baru

[6] Asri Sitompul, *Hukum Internet, Pengenalan Mengenai Masalah Hukum Di Cyberspace* (Bandung: Citra Aditya Bakti, 2001), p. 25.

seperti *cyberstalking*, serangan *online* atau penguntitan berulang-ulang dan ancaman berbahaya[7].

Beberapa kasus terkait pelanggaran data pribadi, mulai dari pencurian data pribadi, kerusakan sistem yang memungkinkan terjadinya pelanggaran data, penyalahgunaan data pribadi yang selama ini diatur dalam bisnis, atau kemungkinan pihak lain yang bisa mengakses data konsumen pribadi. Berdasarkan rekapitulasi data Kementerian Komunikasi dan Informatika Republik Indonesia, per Maret 2020, secara keseluruhan terdapat 44 kasus pelanggaran keamanan informasi, sedangkan kasus turunan yang masih terkait dengan pelanggaran keamanan informasi, dalam hal ini kasus, data pribadi yaitu penipuan berjumlah 9.458 kasus[8].

Salah satu contoh kasus di tengah hiruk pikuk pandemi COVID-19 yang melibatkan startup terkemuka di Indonesia adalah bocornya data pengguna platform Tokopedia, seperti dilansir Kompas.com, sebagai berikut:

"*Data milik 15 juta pengguna Tokopedia diduga bocor di dunia maya. Kabar terbaru menyebutkan data 91 juta pengguna dan lebih dari tujuh juta merchant Tokopedia dijual di situs gelap (dark web). Data tersebut dijual dengan harga 5.000 dollar AS (sekitar Rp 74 juta). Kejadian ini tentu akan merugikan pengguna yang terkena dampak. Email korban berpotensi disalahgunakan untuk kejahatan, misalnya penipuan atau pemerasan. Tokopedia menyadari adanya upaya untuk mencuri data pengguna di platform e-commerce-nya*[9]."

[7] Sujadmiko, "The Urgency of Digital Right Management on Personal Data Protection."

[8] Kementerian Komunikasi dan Informasi, "Statistik Aduan," https://www.kominfo.go.id/statistik, diakses 14 Juni 2021, pukul 15:59 WIB.

[9] Wahyunanda Kusuma Pertiwi, "Data Pengguna Tokopedia Bocor, Cek Apakah Akun Anda Terdampak," 2020, https://tekno.kompas.com/read/2020/05/03/11580057/data-pengguna-tokopedia-bocor-cek-apakah-akun-anda-terdampak, diakses 12 Juni 2021 pukul 16:01 WIB.

Menariknya, saat pandemi COVID-19 yang melanda Indonesia yang berlangsung sejak awal tahun 2020, data pribadi pasien COVID-19 juga tersebar luas dengan begitu mudahnya melalui pesan berantai di berbagai media online seperti Whatsapp dan Facebook. Data pribadi yang tersebar ini meliputi nama lengkap, umur, alamat tempat tinggal, bahkan menampilkan foto profil orang yang bersangkutan. Selain menyebabkan data pribadi pasien yang bersangkutan rentan disalahgunakan oleh pihak yang tidak bertanggung jawab, di sisi lain secara psikologis membuat pasien stres dan terganggu mentalnya. Hal ini tentu menimbulkan efek psikologis, dimana diharapkan seseorang dapat pulih secara fisik bahkan lebih sakit karena penyakit pikiran dan mentalnya serta efek stres yang menimbulkan reaksi emosional yang meliputi kecemasan, kemarahan, dan agresi, serta apatis. dan depresi[10].

Dalam konteks perlindungan data, penting untuk membedakan antara data yang diperoleh secara sah tetapi disalahgunakan dan data yang dikumpulkan secara ilegal (misalnya tanpa persetujuan) atau dicuri (melalui peretasan komputer). Pencurian data umumnya melibatkan serangan siber atau pengambilan data dengan cara lain di mana subjek data tidak menyadari pengumpulan atau modifikasi data mereka. Sedangkan istilah penyalahgunaan data biasanya diterapkan pada data pribadi yang pada awalnya secara sukarela dan sah diberikan oleh pelanggan kepada suatu perusahaan, tetapi kemudian digunakan (baik oleh perusahaan atau pihak ketiga) untuk tujuan yang berada di luar cakupan alasan yang sah.

Informasi pribadi berbentuk metadata yang dikumpulkan oleh seseorang, baik bersifat sukarela maupun wajib, untuk beragam peruntukan disimpan sebagai data digital oleh pihak kedua. Padahal metadata ini amat

[10] Fenty Usman Puluhulawa, Jufryanto Puluhulawa, and Moh. Gufran Katili, "Legal Weak Protection of Personal Data in the 4.0 Industrial Revolution Era," *Jambura Law Review* 2, no. 2 (2020): 182–200.

rentan dicuri atau disalahgunakan oleh pihak ketiga demi tujuan-tujuan yang menguntungkannya. Untuk itu, kebutuhan untuk mengatur informasi pribadi ini penting karena data pribadi menyangkut hak privasi seseorang. Konsep privasi adalah gagasan untuk menjaga integritas pribadi dan martabat kemanusiaan. Selain itu, secara fundamental, data pribadi bisa bernilai ekonomis bagi pihak ketiga yang memang punya peluang untuk memanfaatkannya.

Data pribadi bisa diartikan sebagai semua informasi yang berkaitan dengan identitas seseorang. Bisa jadi ekspresi fisiknya, fisiologis, genetik, psikis, ekonomi, budaya dan identitas social[11]. Data pribadi juga memuat informasi yang bersifat privat yang membedakan karakteristiknya dengan orang lain. Hingga ketika kita berbicara tentang data pribadi, kita mengacu pada semua data atau informasi yang secara langsung atau tidak langsung dapat dikaitkan dengan orang perorangan atau badan hukum[12].

Dalam Pasal 1 Nomor 27 Peraturan Pemerintah No. 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik dan Pasal 1 Nomor 1 Peraturan Menteri Komunikasi dan Informatika No. 20 Tahun 2016[13] tentang Perlindungan Data Pribadi Dalam Sistem Elektronik menyebutkan bahwa yang disebut sebagai data pribadi ialah:

> "*Data pribadi adalah data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya*."

[11] Nicola Boccella, Riccardo Misuraca, and Pierpaolo Tudisco Thor, "The Protection of Personal Data," *International Journal of Technology for Business (IJTB)* 2, no. 1 (n.d.): 43–54.

[12] Ibid.

[13] Pengaturan perlindungan data pribadi dalam hukum nasional diatur secara eksplisit dalam Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang perlindungan data pribadi. Namun Undang-undang ini belum memuat aturan perlindungan data pribadi yang ketat dan komprehensif.

Data individu merupakan informasi yang dapat diandalkan dan berwujud yang melekat dan dapat diidentifikasi, baik langsung maupun tidak langsung, pada setiap orang yang pemanfaatannya mengikuti ketentuan hukum dan peraturan. Dengan kata lain, saat kita berbicara tentang data pribadi, kita merujuk pada semua data atau informasi yang secara langsung atau secara tidak langsung dapat diasosiasikan dengan orang atau badan hukum. Data non-pribadi, sebaliknya, adalah informasi yang dikumpulkan anonim dan tidak dapat digunakan untuk mengidentifikasi orang tertentu[14].

Data disebut sebagai informasi pribadi bila berisi segala informasi yang berhubungan dengan individu hingga dapat dipakai guna mengidentifikasi individu tersebut. Segala atribut yang dapat diidentifikasi, baik secara langsung atau tidak langsung, dengan referensi khusus pada tanda pengenal seperti nama, nomor identifikasi penduduk, atau karakteristik fisik, fisiologis, genetik, mental, ekonomi, budaya atau identitas sosialnya disebut sebagai informasi yang bersifat pribadi. Ringkasnya, data pribadi merupakan data milik individu (*privacy rights*) yang harus dijaga kerahasiaannya serta dilindungi privasinya.

Dalam prakteknya, data pribadi tidak boleh dikumpulkan untuk tujuan-tujuan yang melawan hukum. Artinya pengumpulan data pribadi harus dikaitkan dengan maksud yang relevan pada tujuan awal aktivitas tersebut[15]. Konsekuensi hukumnya, sesuai Pasal 26 UU ITE, data pribadi tersebut tidak boleh dikelola ataupun disebarkan tanpa persetujuan pemilik data tersebut. Dalam hal ini subjek data berhak memperoleh konfirmasi perihal pengelolaan datanya.

---

[14] Boccella, Misuraca, and Thor, "The Protection of Personal Data."

[15] Sinta Dewi, "Prinsip-Prinsip Perlindungan Data Pribadi Nasabah Kartu Kredit Menurut Ketentuan Nasional Dan Implementasinya," *Sosiohumaniora* 19, no. Vol 19, No 3 (2017): SOSIOHUMANIORA, NOPEMBER 2017 (2017): 206–212, http://jurnal.unpad.ac.id/sosiohumaniora/article/view/11380/6971.

Selanjutnya, semua pihak harus mengetahui tentang kondisi yang diperlukan untuk mengumpulkan dan menggunakan data pribadi personal dari pengguna. Secara umum, dalam melakukan segala aktivitasnya, setidaknya ada tiga prinsip yang harus dilakukan, yaitu pembatasan tujuan, minimalisasi data dan transparansi. Yang dimaksud pembatasan tujuan adalah prinsip ini meniscayakan bahwa segala aktivitas pengumpulan dan pemanfaatan data hanya diperbolehkan untuk penggunaan atau tujuan yang jelas yang dinyatakan dalam kontrak. Segera setelah proses penggunaan data berakhir, pihak penerima data berkewajiban untuk sesegera mungkin menghapus semua data pribadi.

Prinsip dasar kedua adalah limitasi atau meminimisasi penggunaan data. Artinya setiap situs web atau penerima data hanya boleh mengumpulkan data pribadi atau konsumen sesedikit mungkin selama aktivitas transaksi. Akibatnya, pemrosesan data pribadi yang tidak diizinkan oleh pemilik data tidak akan diproses dalam tahap selanjutnya. Sedangkan prinsip transparansi menyatakan setidaknya pihak penerima data harus menginformasikan pada pengirim data tentang penggunaan atau pemrosesan data lainnya dan bagaimana data tersebut diproses dan akan digunakan di masa mendatang[16].

Yang perlu diantisipasi sebenarnya ialah bila akumulasi kumpulan data pribadi tersebut disalahgunakan guna lebih mempermudah proses pengidentifikasian yang berujung justru pada potensi membahayakan pribadi-pribadi tersebut. Hal demikian bisa saja terjadi bila pemilik data mengetahui bahwa informasi pribadinya yang telah dikumpulkan pada pihak pengelola data namun justru digunakan oleh pihak lain guna tujuan-tujuan yang bersifat membahayakan, mengganggu bahkan mengancam pihak lain. Disinilah pentingnya kebijakan privasi (*privacy policy*) bagi pengelola data guna menghindari aksi pelanggaran terhadap privasi seseorang.

[16] Boccella, Misuraca, and Thor, "The Protection of Personal Data."

Risiko kejahatan dunia maya yang dapat ditimbulkan dari bocornya data pribadi pengguna adalah[17]:

1. Pemasaran jarak jauh. Data nomor telepon dapat dipertukarkan sehingga tidak heran jika kita mendapatkan telepon atau SMS dengan penawaran produk/jasa berhadiah;

2. Model Penipuan Penipuan Phishing. Penipuan dengan memastikan bahwa pengguna memenangkan hadiah tertentu yang diperoleh jika mereka memberikan sejumlah uang atau mengarahkan pengguna untuk memberikan data pribadi sambil menunjuk ke situs palsu;

3. Perincian layanan lainnya. Data yang bocor dapat digunakan untuk mengakses akun di layanan sosial/online terintegrasi lainnya seperti Go Pay, Instagram, dll;

4. Membongkar kata sandi / kata sandi. Tanggal lahir dan email yang bocor juga bisa menjadi modal hacker untuk mengambil alih akun;

5. Digunakan untuk membuat akun pinjaman online secara diam-diam. Penjahat juga bisa mengajukan pinjaman di aplikasi pinjaman online dengan data yang bocor;

6. Pembuatan profil untuk target politik atau iklan media social. Data pribadi yang diambil dapat digunakan untuk rekayasa sosial hingga pembuatan profil yang menghasilkan penggerak opini publik.

[17] CNN Indonesia, "6 Bahaya Yang Intai Usai Kasus Data Bocor Tokopedia-Bukalapak," *2020*, n.d., https://www.cnnindonesia.com/teknologi/20200506105640-185-500591/6-bahaya-yang-intai-usai-kasus-data-bocor-tokopedia-bukalapak, diakses 12 Juni 2021 pukul 16:12 WIB.

Diantara kejahatan digital yang melanggar privasi berupa informasi data pribadi ialah sebagai berikut:

1. Hacking atau peretasan adalah upaya untuk memodifikasi, menganalisis dan menerobos masuk ke dalam system jaringan computer[18]. Kasus hacking ini terhitung sering terjadi di ruang siber[19]. Pelaku peretasan seringkali mengubah atau merusak homepage guna mengambil data-data tertentu yang dinilai penting oleh hacker.

2. Cracking, adalah jenis kejahatan pencurian data yang dilakukan dengan menyusup ke dalam sistem jaringan internet dengan tanpa izin dengan tujuan mengambil data-data penting pemilikinya. Karakteristik cracking adalah kerusakan sistem yang mengakibatkan tidak dapat berfungsi. Adapun tahapannya adalah sebagai berikut: *footprinting* (pencarian data atau informasi pada system yang disusupi), *scanning* (pemilihan sasaran korban), *enumerasi* (pencarian data pribadi atau *user account* yang menjadi sararan), *gaining access* (upaya pengaksesan dalam system yang disasar), *escalating privilege* (*cracker* menaikkan posisinya menjadi admin atau *root*), *pilfering* (tahap pencurian data cleartext password di config file, registry, dan user data), *covering tracks* (penutupan jejak digital), *creating backdoors*

[18] Bambang Hartono, "Hacker Dalam Perspektif Hukum Indonesia," *Masalah Masalah Hukum*, no. 26 (2011): 23–30.

[19] B. Suhariyanto, *Tindak Pidana Teknologi Informasi (Cyber Crime) Urgensi Pengaturan Dan Celah Hukumnya* (Jakarta: Rajawali Press, 2014), p. 18.

(pembuatan jalur pintas guna masuk kembali dalam sistem) dan *denial of service* (upaya terakhir berupa pelumpuhan system)[20].

3. Carding, aktivitas transaksi internet dengan menggunakan nomor ataupun identitas kartu kredit orang lain secara illegal. Problem cybercrime yang sering muncul di Indonesia bermula dari "carder" yang berfungsi mengintip kartu kredit lalu pelaku mencuri informasi tabungan nasabah di bank demi keuntungan pribadinya[21].

4. Cyber sabotage, sesuai penamaannya, pelaku melakukan sabotase guna mengganggu, merusak bahkan menghancurkan data pada jaringan computer yang terhubung dengan internet. Kejahatan digital ini seringkali dilakukan dengan penyusupan virus computer atau melalui program tertentu hingga jaringan computer tidak bisa berfungsi sebagaimana mestinya[22].

5. Spyware, suatu program yang diinisiasi guna merekam semua aktivitas calon korban di dunia siber ataupun memanipulasi tampilan laman virtualnya[23]. Data yang tersimpan tersebut akan dijual ke perusahaan-perusahaan yang berminat memasang iklan ataupun menyebarkan virus computer.

6. Phising scam

---

[20] Nur Khalimatus Sa'diyah, "Modus Operandi Tindak Pidana Cracker Menurut Undang-Undang Informasi Dan Transaksi Elektronik," *Perspektif* 17, no. 2 (2012): p. 83.

[21] Ineu Rahmawati, "The Analysis Of Cyber Crime Threat Risk Management To Increase Cyber Defense," *Jurnal Pertahanan & Bela Negara* 7, no. 2 (2017): 51–66.

[22] A. Aco Agus and Riskawati, "PENANGANAN KASUS CYBER CRIME DI KOTA MAKASSAR (Studi Pada Kantor Kepolisian Resort Kota Besar Makassar)," *Jurnal Supremasi* 11, no. 1 (2016): 20–29.

[23] Rahmawati, "The Analysis Of Cyber Crime Threat Risk Management To Increase Cyber Defense."

Phishing dan munculnya virus Trojan (mereka digunakan untuk mencuri data tetapi sering dikaitkan dengan virus lain untuk merusak keamanan perangkat) yang mencoba mencuri informasi yang dapat digunakan untuk tujuan yang curang. Phishing adalah aktivitas ilegal yang mengeksploitasi teknik manipulasi psikologis (mempelajari perilaku individu seseorang untuk mencuri informasi), dan digunakan untuk mendapatkan akses ke informasi pribadi atau rahasia untuk tujuan pencurian identitas melalui penggunaan komunikasi elektronik, terutama email palsu atau pesan instan, tetapi juga kontak telepon. Berkat pesan-pesan ini, pengguna tertipu dan diarahkan untuk mengungkapkan data pribadi, seperti nomor rekening bank, nomor kartu kredit, kode identifikasi[24].

Cara kerjanya antara lain: malware pengguna (*phisher*) mengirimkan pesan email kepada pengguna. Email mengundang penerima untuk mengikuti tautan, yang hadir dalam bentuk pesan. Tautan yang diberikan, bagaimanapun, tidak benar-benar mengarah ke situs web resmi, tetapi berupa salinan fiktif yang mirip dengan situs resmi yang terletak di server yang dikendalikan oleh *phisher*. Pesan tersebut meminta dan memperoleh data pribadi tertentu dari penerima, biasanya dengan alasan konfirmasi atau kebutuhan untuk membuat otentikasi ke sistem. Informasi ini disimpan oleh server yang dikelola oleh *phisher*.

7. Pharming

Pharming adalah teknik cracking yang digunakan untuk mendapatkan akses ke informasi pribadi dan rahasia untuk berbagai

[24] Boccella, Misuraca, and Thor, "The Protection of Personal Data.", p. 50.

tujuan. Berkat teknik ini, pengguna tertipu dan tanpa sadar mengungkapkan kepada orang asing data sensitif mereka, seperti nomor rekening bank, nama pengguna, kata sandi, nomor kartu kredit, dll. Tujuan akhir dari pharming adalah sama dengan phishing, yaitu mengarahkan korban ke server web "kloning" yang dilengkapi khusus untuk mencuri data pribadi korban.

Sementara di Indonesia, belum ada peraturan yang secara tegas dan spesifik mengatur tentang pelaku pembobol data pribadi. Sebagai perbandingan, diantara Negara yang telah memberlakukan perlindungan data pribadi ialah Malaysia yang telah menerbitkan *Digital Signature Act* pada tahun 1997. Kemudian pada Mei 2010, Malaysia mengesahkan *Personal Data Protection Act* (PDPA). Melalui PDPA ini, privasi warga Malaysia dalam konteks transaksi komersial resmi dilindungi oleh undang-undang[25]. Dalam Pasal 6 PDPA terdapat prinsip umum yang berisi pengguna data tidak boleh mengolah data pribadi kecuali bila pemilik data telah memberikan persetujuan.

Belanda juga memiliki peraturan mengenai data pribadi yang diketahui sebagai *Wet Bescherming Persoongegevens*. Kemudian Belgia telah memiliki regulasi mengenai perlindungan data pribadi sejak tahun 1992, kemudian pada tahun 2018 Pemerintah Belgia telah mengganti peraturan yang disebut *The Belgian Law of July 2018* tentang perlindungan orang perseorangan sehubungan dengan pemrosesan data pribadi[26]. Pada tahun 1998, Amerika Serikat juga telah

[25] Muh. Firmansyah Pradana, "Perlindungan Hukum Terhadap Pengguna Cloud Computing Atas Privasi Dan Data Pribadi" (Tesis Program Studi Magister Kenotariatan Fakultas Hukum Universitas Hasanuddin Makassar, 2018), p. 39.

[26] Haganta, "Legal Protection of Personal Data As Privacy Rights Of E-Commerce Consumers Amid The Covid-19 Pandemic. p. 77-90.",

mengeluarkan kebijakan *Digital Millennium Copyright Law* sebagai bentuk penghargaan atas privasi seseorang[27].

Indonesia bisa dikatakan tertinggal dibanding Negara-negara lain dalam merumuskan peraturan perundangan terkait perlindungan data pribadi. Setidaknya, sampai saat ini, Indonesia belum mempunyai peraturan perundangan yang mengatur secara spesifik terkait perlindungan data pribadi.

Kemudian perlahan Pemerintah menunjukkan kepeduliannya terhadap informasi pribadi melalui diterbitkannya Permenkominfo 20/2016, UU ITE, PP PSTE, dan PP PMSE yang secara khusus mengatur e-commerce, meski masih terdapat ketidakjelasan norma makna data pribadi yang diatur dalam PP. PMSE dan PP PSTE dan UU Administrasi Kependudukan. Setidaknya terdapat tiga puluh dua undang-undang yang secara substansi membahas perlindungan informasi pribadi namun masih bersifat sectoral dan parsial hingga perlindungan terhadap data pribadi masih belum optimal[28]. Tiga undang-undang tersebut dikeluarkan oleh Kementerian Kesehatan, Kementerian Kominfo dan Kementerian Dalam Negeri.

Tujuan dari diperlukannya kerangka hukum adalah untuk menghindari pelanggaran tersebut oleh memastikan seseorang mendapatkan perlindungan yang memadai dan memproteksi konsumen dengan terus memantau aktivitas yang ada dalam transaksi digital. Hal ini dikarenakan penyalahgunaan informasi pribadi dapat dikategorikan sebagai perbuatan yang memenuhi unsur pidana, hingga diperlukan peraturan perundangan yang memuat sanksi yang tegas bagi pelakunya.

---

[27] Soediro, "Prinsip Keamanan, Privasi, Dan Etika Dalam Undang-Undang Informasi Dan Transaksi Elektronik Dalam Perspektif Hukum Islam," *Kosmik Hukum* 18, no. 2 (2018): 95–112.

[28] Fanny Priscyllia, "Perlindungan Privasi Data Pribadi Dalam Perspektif Perbandingan Hukum," *Jatiswara* 34, no. 3 (2019): p. 248.

Konsep perlindungan data pribadi ini amat erat kaitannya dengan hak privasi seseorang. Perlindungan data pribadi biasanya berpusat pada mengamankan informasi dan termasuk enkripsi, protokol komunikasi yang aman dan kebijakan keamanan yang terukur. Fokus dari perlindungan data adalah keamanan, sedangkan privasi data lebih berkaitan dengan bagaimana informasi diatur dan digunakan.

Perlindungan ini bertujuan untuk melindungi nilai-nilai yang fundamental, yaitu otonomi dan kemanusiaan martabat seseorang, dengan memberikan lingkup pribadi dimana ia dapat dengan bebas mengembangkan aktivitas sekaligus menjaga harkatnya. Bisa dibilang, kuncinya adalah keamanan *cyber* hingga membentuk ekosistem digital baru yang nyaman, terjamin kerahasiaannya, tanpa risiko pembobolan privasi dan pelanggaran hak-hak dasar sebagai warga Negara, serta saling menghargai etika digital.

Diantara kelebihan adanya peraturan perlindungan data pribadi ialah[29]:

1) Kepastian hukum, karena privasi atas data pribadi secara tegas dianggap sebagai hak dasar yang harus dilindungi oleh Negara.
2) Mengatur secara ketat kegiatan pemerintah dan sektor swasta;
3) Sesuai untuk negara yang memiliki sistem hukum *civil law* yang menempatkan perundang-undangan sebagai salah satu sumber utama hukum;
4) Konsep regulasi ini cocok bagi negara yang belum memiliki Undang-Undang Privasi tentang Perlindungan Data Pribadi karena memuat prinsip dan mekanisme kunci yang harus dilakukan untuk melindungi privasi atas informasi data pribadi.

[29] Sinta Rosadi, "Protecting Privacy On Personal Data In Digital Economic Era : Legal Framework In Indonesia," *Brawijaya Law Journal* 5, no. 2 (2018): 143–157.

Oleh karena itu, peraturan perundangan yang mengatur perlindungan data pribadi harus segera dibentuk untuk melindungi informasi pribadi agar tidak disalahgunakan dan dimanipulasi. Selain melanggar etika publik, pengumpulan data yang disalahgunakan dapat dikategorikan sebagai pelanggaran hak privasi yang dilindungi oleh konstitusi kita.

Untuk alasan inilah, pengusaha atau pembuat situs web wajib menjaga perlindungan data pribadi, baik untuk kepentingan pelanggan mereka dan untuk menghindari konsekuensi hukum. Diperlukan analitis mitigasi resiko secara syar'i demi terhindar dari kejahatan pencurian dan penyalahgunaan data pribadi di ruang siber yang disebut *sadd dzari'ah*. Metode hukum Islam ini bekerja dengan cara memblokir segala perantara yang mengundang kemadharatan demi mewujudkan kemaslahatan bersama.

Sadd dzari'ah merupakan salah satu metode istinbath hukum Islam yang berorientasi pada terpeliharanya kemaslahatan. Secara etimologi, *sadd* berarti menutup, mencegah, melarang. Sementara *dzari'ah* diartikan sebagai prasarana atau perantara sesuatu. Atau menurut Ibn Qayyim disebut sebagai hal-hal yang menjadi perantara dan jalan menuju sesuatu[30]. Sementara dalam ushul fiqh, *dzari'ah* lebih dimaknai sebagai segala sesuatu yang dapat menjadi perantara hal yang dilarang secara syar'i hingga harus dilarang[31]. Metode ini terhitung preventif, artinya segala hal yang awalnya bernilai mubah bisa berubah menjadi terlarang dengan berdasarkan indikasi-indikasi yang kuat sebab mengingat efek yang ditimbulkannya.

Sadd dzari'ah berarti sarana untuk mencapai tujuan tertentu, sedangkan secara harfiah berarti pemblokiran. *Sadd dzari'ah* dengan demikian menyiratkan

[30] Muhammad bin Abi Bakar Ayyub Azzar'i Abu Abdillah Ibnul Qayyim Al-Jauzi, *I'lamul Muwaqin*, Jilid 5., n.d. p. 496.

[31] Wahbah al Zuhaily, *Ushul Fiqh Al Islamy*, Juz II. (Dar al-Fikr, 1986), p. 873.

pemblokiran sarana menuju yang diharapkan kejahatan, yang mungkin terwujud jika sarana menuju itu tidak terhalang. Metode ini berlaku ketika ada konflik antara cara dan tujuan pada skala nilai cara yang sebenarnya mubah namun tujuannya diharamkan. *Sadd dzari'ah* memiliki potensi besar untuk digunakan untuk memblokir sarana untuk kerugian publik tertentu (mafsadah) atas nama kemaslahatan bersama.

Cara pandang syar'i dalam memahami risiko kemafsadatan dalam pelanggaran data-data pribadi dapat dilakukan dengan menggunakan metode *sadd dzari'ah* yang mempertimbangkan aspek mafsadat dan maslahat. Metode ini berusaha menjauhkan seseorang dari potensi kemaksiatan sekaligus memudahkan pencapaian kemaslahatan.

Mayoritas ulama termasuk Imam al-Syafi'i mengakui *sadd dzari'ah* sebagai salah satu sumber ijtihad, bahkan ada perselisihan kecil dan namanya hanya tentang bentuk atau cara menggunakannya, dan itu tidak mengubah kesepakatan mereka dalam bentuk umum. *Sadd al-dzari'ah*, sebagaimana ungkapan Wahbah Zuhaili, ialah metode pengambilan hokum yang bersifat mencegah segala sesuatu, baik perkataan maupun perbuatan, yang dapat menyampaikan pada hal yang dilarang secara syar'i, yang mengandung kerusakan[32]. Urgensi *sadd dzari'ah* ialah agar segala bahaya dihilangkan (*ad-dhararu yuzalu*) guna tercapainya kemaslahatan sebagai realisasi dari tujuan syari'at. Hingga Ibn Qayyim menyatakan bahwa pada hakikatnya, *sadd dzari'ah* merupakan seperempat taklif[33].

Menurut Thahir Ibn Asyur, *sadd dzari'ah* bisa juga dipahami sebagai istilah (*laqab*) yang digunakan oleh para ahli fiqh terkait metode pendekatan hukum yang berfungsi membatalkan, mencegah bahkan melarang tindakan yang

[32] Wahbah Al-Zuhayliy, *Al-Wajiz Fi Usul Al-Fiqh* (Damaskus: Dar al-Fikr, 1999), p. 108.

[33] Al-Jauzi, *I'lamul Muwaqin*, Jilid III, p. 171.

awalnya tidak mengandung unsur kerusakan, karena dianggap menyebabkan kerusakan yang disepakati[34]. Titik tumpu metode ini adalah pada konsistensi dalam menjaga ketentuan-ketentuan syari'ah dengan memitigasi segala upaya negatif guna mencapai tujuan, bahkan sebelum resiko itu benar-benar terjadi. Upaya pengekangan ini bertujuan lebih spesifik, yaitu menolak resiko buruk dan menjaga kemaslahatan.

Sementara Imam Qarafi membagi *sadd dzari'ah* ini dalam tiga bagian. *Pertama*, sarana terhadap sesuatu yang telah disepakati dilarang, seperti perbuatan seseorang yang mencaci berhala dimana ia meyakini bahwa penyembah berhala akan membalas tindakannya tersebut. *Kedua*, sarana yang sejatinya tidak terlarang namun bisa menimbulkan potensi terjadinya tindakan yang dilarang, misalnya, tindakan menanam anggur yang bisa berpotensi dijadikan *khamr*. *Ketiga*, hal yang masih terjadi selisih pendapat antara diperbolehkan atau dilarang, semisal tindakan melihat perempuan yang bisa menimbulkan potensi terjadinya zina[35].

Asy-Syatibi sendiri membagi *sadd dzari'ah* menjadi empat macam[36]. *Pertama*, efek kerusakan yang akan ditimbulkan bersifat definitif (*qath'i*). Misalnya bila seseorang hendak menggali sumur di depan rumahnya yang ia sendiri tahu akan ada tamu yang berkunjung padanya di malam hari. Perbuatannya menggali sumur tersebut yang awalnya diperbolehkan menjadi terlarang karena sudah pasti akan mendatangkan kemafsadatan.

Kedua, efek kerusakan yang akan ditimbulkan bersifat dugaan kuat. Dalam keadaan ini anggapan yang kuat sama dengan suatu kepastian. Contohnya

---

[34] Muhammad Thahir Ibn Asyur, *Maqasid Syari'ah Al-Islamiyyah* (Petaling Jaya Malaysia: Dar An-Nafais, 2001), p. 365.

[35] Muhammad Hisyam Al Burhani, *Sadd Al Dzari'ah Fi Al-Syari'ah Al Islamiyyah* (Dar Kutub Ilmiyyah, n.d.), p. 105.

[36] Al Syatibi, *Al Muwafaqat*, Juz III. (Mesir: Matba'ah al Maktabah al Tijariyah, n.d.), p. 358-361.

adalah bila seseorang menjual anggur kepada perusahaan minuman keras. Hukum asal menjual anggur adalah diperbolehkan namun ketika dijual pada perusahaan minuman keras menjadi terlarang karena diduga kuat akan diproduksi menjadi minuman keras yang memabukkan.

Ketiga, efek kerusakan yang akan ditimbulkan bersifat kecil kemungkinannya. Hal ini karena keuntungan yang diperoleh dari perbuatan tersebut lebih besar daripada kerugian yang mungkin timbul sebagai akibat sampingan dari perbuatan tersebut. Misalnya seseorang yang mengemudikan kendaraan bermotor dengan kecepatan 60 km/jam di jalur dan kondisi normal. Contoh lainnya adalah praktek jual beli secara kredit yang dapat menimbulkan resiko terjerat riba.

Keempat, efek kerusakan yang akan ditimbulkan bersifat sangat jarang kemungkinannya. Perbuatan yang kebanyakan efeknya mengarah pada mafsadah tetapi tidak sampai pada tingkat asumsi yang kuat. Contohnya menjual benda-benda tajam seperti pisau, gunting, celurit di malam hari. Para fuqaha sepakat bahwa *dzari'ah* tipe pertama dan kedua harus dilarang. Namun untuk tipe ketiga dan keempat, terjadi perbedaan pendapat di kalangan para ulama.[37] Penerimaan *sadd dzari'ah* oleh Imam al-Syafi'i sendiri secara tidak langsung lebih umum dan terbatas pada perbuatan yang diyakini mengarah pada lebih mafsadah, tetapi perbuatan itu tidak sampai kepada tingkat praduga kuat[38].

Model-model *sadd dzari'ah* di atas setidaknya dapat dikenali melalui tiga hal, yaitu motif pelaku, efek yang ditimbulkannya dan tujuan perbuatannya[39]. Bila

[37] Zuhaily, *Ushul Fiqh Al Islamy,* Juz II, p. 877-883.

[38] Ahmad Dahlan Salleh et al., "Theory and Application of Sadd Al-Dhara'i' (Blocking the Means) in Shafi'iyya School," *International Journal of Academic Research in Business and Social Sciences* 9, no. 1 (2019): 724–737.

[39] Intan Arafah, "Pendekatan Sadd Adz-Dzari'ah Dalam Studi Islam," *Al - Muamalat: Jurnal Hukum dan Ekonomi Syariah* 5, no. 1 (2020): 68–86.

motif, efek dan tujuan perbuatannya kebaikan, maka tindakan tersebut bernilai diperbolehkan. Namun bila sebaliknya, maka status hukumnya terlarang secara syara'. Kedudukan *sadd dzari'ah* sebagai salah satu metode istinbath hukum karena *washilah* dianggap sebagai mukaddimah dari suatu perbuatan, maka hal demikian menjadi petunjuk bahwa *washilah* itu sebagaimana hukum yang ditetapkan oleh syara' terhadap pokok perbuatannya.

Tujuan dari kerangka ushuliyyah *sadd dzari'ah* adalah untuk menghindari pelanggaran tersebut dengan memastikan konsumen mendapatkan perlindungan yang memadai dan dengan terus memantau aktivitas yang ada dalam transaksi digital. Hal ini dikarenakan secara umum, syari'at Islam ditujukan pada terwujudnya aspek kemaslahatan ataupun menghindari unsur kemadharatan. Konsekuensi logisnya, segala hal yang patut diduga sebagai sarana yang mendatangkan kemafsadatan haruslah dihalangi karena bernilai haram.

Penetapan hukum melalui *sadd dzari'ah* adalah menghitung dampak dan akibat dari suatu perbuatan ketika telah dilakukan dan tidak hanya melihat motif atau niat pelakunya. Oleh karena itu, jika suatu perbuatan mengarah pada sesuatu yang menjadi mafsadah dan merugikan umat manusia, maka hal itu dilarang karena menurut hukum Islam metode fikih yaitu tolak kerugiannya lebih utama.

Bila dianalisis, data pribadi bila tidak dilindungi oleh Negara maka bisa masuk dalam kategori kedua dalam pembagian Imam Syatibi di atas, yaitu bila tidak diproteksi besar kemungkinan akan membawa pada kemafsadatan. Dari sinilah arti penting illat hukum, bahwa pergeseran empat kemungkinan resiko tersebut tergantung pada perbedaan cara pandang terhadap illat itu sendiri. Hal ini dikarenakan metode *sadd dzari'ah* tidak terlepas dari cara pandang terhadap akibat yang ditimbulkan dari suatu perbuatan mukallaf. Perbedaan dalam menilai

sarana, alat dan atau *wasilah* itulah yang menentukan nilai hukum dari suatu tindakan[40].

Aplikasi dalam *sadd dzari'ah* ialah bila seseorang melakukan suatu kegiatan/perilaku yang terkait pengumpulan data pribadinya yang semula diperbolehkan karena mengandung kemanfaatan, tetapi dalam tujuan yang akan dicapainya berpotensi dapat berakhir dengan kerugian dan kemafsadatan bila tanpa adanya perlindungan dari Pemerintah. Oleh karena itu, dibutuhkan adanya kebijakan perlindungan data pribadi sebagai langkah preventif guna mencegah kemafsadatan (*sadd dzari'ah*), terjadinya penyalahgunaan dalam pengelolaan data pribadi. Upaya perlindungan data pribadi menjadi mutlak dibutuhkan karena bila tidak diatur dalam bentuk perundang-undangan akan mengakibatkan potensi tersebarnya data pribadi seseorang.

Data-data pribadi haruslah diproteksi karena secara actual maupun potensial dapat merusak harkat dan martabat kemanusiaan seseorang. Hingga melindungi informasi yang bersifat pribadi merupakan kebutuhan primer (*hajat dharuriyat*) karena tergolong dalam maqashid syari'at, yaitu prinsip perlindungan kehormatan diri (*hifdzul 'irdh*).

Penyebarluasan data pribadi merupakan bentuk kerusakan (*mafsadat*) perlindungan terhadap kehormatan (*hifzh al-irdh*) yang menimbulkan bahaya. Bahaya yang timbul berupa hilangnya harkat dan martabat seseorang, bahkan dapat mengakibatkan hancurnya *dharuriyat al khams* karena berawal dari harga diri sebagai hak dasar seseorang yang hilang. Padahal dalam hukum Islam, potensi bahaya harus dihilangkan,

[40] Nurdhin Baroroh, "Metamorfosis Illat Hukum Dalam Sad Adz-Dzari'ah Dan Fath Adz-Dzari'ah," *Al-Mazahib* 5, no. 2 (2017): 289–304.

Diantara dalil larangan menjauhi perbuatan yang awalnya dibolehkan namun dapat mendatangkan kerusakan ialah:

وَلَا تَسُبُّوا الَّذِينَ يَدْعُونَ مِنْ دُونِ اللَّهِ فَيَسُبُّوا اللَّهَ عَدْوًا بِغَيْرِ عِلْمٍ ۗ

Artinya; "*Dan juga kamu memaki sesembahan yang mereka sembah selain Allah, karena nanti mereka akan memaki Allah dengan melampaui batas tanpa pengetahuan"* (Q.S. Al-An'am: 108).

Dalam ayat di atas, Allah SWT melarang umat Islam untuk memperolok berhala sesembahan mereka, sebab hal ini mampu menutup sarana ke arah tindakan kaum musyrik mencaci Allah SWT.

Rasulullah SAW juga pernah bersabda:

وعن ابي هريرة رضي الله عنه قال قال رسول الله صلى الله عليه وسلم المسلم اخو المسلم لا يخونه ولا يكذبه ولايخذله كل المسلم علي المسلم حرام عرضه وماله ودمه التقوى ههنا بحسب امرئ من الشر ان يحقر اخاه المسلم (رواه الترمذي)

Artinya: Dari Abu Hurairah, dia berkata: "*Nabi bersabda, sesama Muslim adalah saudara, sesama Muslim tidak boleh mengkhianati, menipu dan menghina mereka, sesama muslim haram kehormatan, harta dan darah mereka, takwa ada di sini (sembari menunjuk dadanya). Cukuplah seseorang itu dalam kejelekan selama dia merendahkan saudaranya sesama muslim*."

Dalam kaidah fiqh juga diterangkan bahwa prasarana sesuatu hal dihukumi sama dengan hukum tujuan perbuatan.

للوسائل حكم المقاصد

Artinya: "*Wasilah (perantara) itu hukumnya adalah sebagaimana hukum yang berlaku pada apa yang dituju*".

Setiap perbuatan pasti memiliki tujuan yang akan dicapai. Dalam menggapai tujuan tersebut, seorang mukallaf membutuhkan media yang menjadi perantara. Dengan demikian, dapat dipahami bahwa status hukum media itu harus sama nilainya dengan tujuan.

Pada kaidah fikih yang lain disebutkan sebagai berikut:

درء المفاسد اولى من جلب المصالح

Artinya: "*Menolak keburukan (mafsadah) lebih diutamakan daripada meraih kebaikan (maslahah).*"

الضرر يزال

Artinya: "*Kemadharatan (harus) dihilangkan*"

Berdasarkan dalil-dalil di atas, dalam perspektif *sadd dzari'ah*, bahaya penyebaran data pribadi harus dihilangkan. Perlindungan data pribadi harus dilindungi oleh semua pihak, baik nasabah fintech, peer to peer lending, penyelenggara fintech, dan Pemerintah.

Setidaknya ada empat alasan utama mengapa Indonesia sangat urgen memiliki peraturan perundangan yang lebih spesifik terkait perlindungan data pribadi. *Pertama*, banyak kasus penyalahgunaan data pribadi pengguna internet, seperti penggunaan media sosial, internet banking, layanan publik yang sangat merugikan pemilik data pribadi. *Kedua*, Uni Eropa memberlakukan *General Data Protection Regulation* (GDPR) pada 25 Mei 2018. Yang mana aturan ini berlaku

secara internasional untuk perusahaan mana pun yang menargetkan penduduk Benua Eropa[41].

Ketiga, jika upaya pengumpulan data yang semakin massif di era digital ini tidak diimbangi dengan penghargaan akan hak privasi warga sebagai individu maka yang terjadi justru pengesampingan hak-hak konstitusional warga Negara. Hal ini sebagaimana yang termaktub dalam Pasal 28 G Undang-Undang Dasar 1945 yang menjelaskan bahwa perlindungan informasi pribadi merupakan amanah konstitusi yang di dalamnya menjunjung tinggi nilai-nilai Hak Asasi Manusia agar Negara hadir guna memberikan jaminan keamanan privasi terhadap warganya.

Keempat, urgensi yuridis mengenai perlindungan data pribadi dapat dilihat bahwa perlindungan data pribadi adalah bagian dari hak asasi manusia yang diatur pada Pasal 12 Deklarasi Universal Hak Asasi Manusia (DUHAM) yang memberi landasan yuridis bagi negara-negara anggotanya terkait kewajiban sebuah negara secara yuridis konstitusional untuk membentuk instrument hukum guna melindungi privasi warga negaranya.

Selain itu, secara legal-formal, dalam hak atas informasi pribadi termuat dalam beberapa instrumen hak asasi manusia, diantaranya ialah[42]:

a. Deklarasi Umum HAM PBB (United Nations Declaration of Human Rights/UDHR) 1948, Pasal 12 berbunyi:

---

[41] Diana Setiawati, Hary Abdul Hakim, and Fahmi Adam Hasby Yoga, "Optimizing Personal Data Protection in Indonesia: Lesson Learned from China, South Korea, and Singapore," *Indonesian Comparative Law Review* 2, no. 2 (2020): p. 106.

[42] Wahyudi Djafar dan Asep Komarudin, *Perlindungan Hak Privasi Di Internet : Beberapa Kata Kunci* (Jakarta: Lembaga Studi dan Advokasi Masyarakat, 2014), p. 33.

"*Tidak seorang pun boleh diganggu urusan pribadinya, keluarganya, rumah tangganya atau hubungan surat menyuratnya dengan sewenang-wenang; juga tidak diperkenankan melakukan pelanggaran atas kehormatan dan nama baiknya. Setiap orang berhak mendapat perlindungan hukum terhadap gangguan atau pelanggaran seperti ini*".

b. Konvenan Internasional tentang Hak Sipil dan Politik (International Convenant on Civil and Political Rights/ ICCPR) 1966, Pasal 17 menyatakan :

" *Tidak boleh seorang pun yang dapat secara sewenang-wenang atau secara tidak sah dicampuri masalah-masalah pribadinya, keluarganya, rumah atau hubungan surat-menyuratnya atau secara tidak sah diserang kehormatan dan nama baiknya. Setiap orang berhak atas perlindungan hukum terhadap campur tangan atau serangan seperti tersebut diatas.*"

Menurut Bygrave, konvensi ini menjadi dasar hukum terkuat dalam hukum internasional hingga negara berkewajiban melindungi privasi warganya melalui peraturan perundang-undangan[43].

Urgensi adanya regulasi terhadap perlindungan data pribadi adalah agar privasi setiap individu dijamin kerahasiaannya oleh peraturan perundangan dan bagi pihak pengumpul data (*data collector*) untuk lebih menghargai informasi pribadi yang telah dikumpulkan dengan tidak menyebarkannya kepada pihak ketiga.

Hal ini sesuai dengan firman Allah dalam surat An-Nur ayat 27

يَٰٓأَيُّهَا ٱلَّذِينَ ءَامَنُواْ لَا تَدۡخُلُواْ بُيُوتًا غَيۡرَ بُيُوتِكُمۡ حَتَّىٰ تَسۡتَأۡنِسُواْ وَتُسَلِّمُواْ عَلَىٰٓ أَهۡلِهَاۚ ذَٰلِكُمۡ خَيۡرٞ لَّكُمۡ لَعَلَّكُمۡ تَذَكَّرُونَ

[43] L. A. Bygrave, "Data Protection Pursuant to the Right to Privacy in Human Rights Treaties," *International Journal of Law and Information Technology* 6, No. 3 Volume 6 (1998): 247–284.

Artinya: *Hai orang-orang yang beriman, janganlah kamu memasuki rumah yang bukan rumahmu sebelum meminta izin dan memberi salam kepada penghuninya. Yang demikian itu lebih baik bagimu, agar kamu (selalu) ingat*. (Q.S. 24: 27).

Upaya perlindungan informasi data pribadi melalui perspektif *sadd dzari'ah* ini sekaligus membuktikan bahwa hukum Islam bekerja berlandaskan pada menjaga eksistensi kemaslahatan bersama. Untuk itu, syari'ah menetapkan metode hukum preventif guna menunjang landasan-landasan kemaslahatan, dengan memblokir segala unsur yang berpotensi menimbulkan kerusakan.

Tabel Klasifikasi Ancaman Data Pribadi Dalam Perspektif Sadd Dzari'ah

No.	Indikator Ancaman	Dzari'ah (Wasail)	Sadd	Tujuan	Sadd Dzari'ah		Maqashid Syari'ah
					Imam Qarafi	Asy-Syatibi	
1.	Hacking	Peretasan data pribadi melalui upaya penyusupan system keamanan jaringan	Pembentukan UU Perlindungan Data Pribadi	Menerobos system jaringan	**Tipe Kedua** (sarana yang sejatinya tidak terlarang namun bisa menimbulkan potensi terjadinya tindakan yang dilarang)	**Tipe Kedua** (efek kerusakan yang akan ditimbulkan bersifat dugaan kuat)	Hifdzul 'Irdh
2.	Cracking	Pencurian data pribadi yang sifatnya lebih anarkis,	Pembentukan UU Perlindungan Data Pribadi	Kerusakan sistem yang mengakibatkan tidak dapat berfungsi	**Tipe Kedua** (sarana yang sejatinya tidak terlarang namun bisa menimbulkan potensi terjadinya tindakan yang dilarang)	**Tipe Kesatu** (efek kerusakan yang akan ditimbulkan bersifat definitif (*qath'i*))	Hifdzul 'Irdh
3.	Carding	Menggunakan nomor ataupun identitas kartu kredit orang lain secara illegal	Pembentukan UU Perlindungan Data Pribadi	Mencuri informasi akun tabungan nasabah	**Tipe Kedua** (sarana yang sejatinya tidak terlarang namun bisa menimbulkan potensi terjadinya tindakan yang dilarang)	**Tipe Kedua** (efek kerusakan yang akan ditimbulkan bersifat dugaan kuat)	Hifdzul 'Irdh
4.	Cyber sabotage	Mengganggu, merusak bahkan	Pembentukan UU	Jaringan computer	**Tipe Kedua** (sarana yang	**Tipe Kesatu** (efek	Hifdzul 'Irdh

		menghancurkan data pada jaringan computer yang terhubung dengan internet	Perlindungan Data Pribadi	tidak bisa berfungsi sebagaiman a mestinya	sejatinya tidak terlarang namun bisa menimbulkan potensi terjadinya tindakan yang dilarang)	kerusakan yang akan ditimbulkan bersifat definitif (*qath'i*))	
5.	Spyware	Merekam semua aktivitas calon korban di dunia siber ataupun memanipulasi tampilan laman virtualnya	Pembentukan UU Perlindungan Data Pribadi	Menjual data pribadi ke perusahaan iklan	**Tipe Kedua** (sarana yang sejatinya tidak terlarang namun bisa menimbulkan potensi terjadinya tindakan yang dilarang)	**Tipe Kedua** (efek kerusakan yang akan ditimbulkan bersifat dugaan kuat)	Hifdzul 'Irdh
6.	Phising scam	Penggunaan komunikasi elektronik, terutama email palsu atau pesan instan, tetapi juga kontak telepon	Pembentukan UU Perlindungan Data Pribadi	Mendapatka n akses ke informasi pribadi atau rahasia untuk tujuan pencurian identitas	**Tipe Kedua** (sarana yang sejatinya tidak terlarang namun bisa menimbulkan potensi terjadinya tindakan yang dilarang)	**Tipe Kedua** (efek kerusakan yang akan ditimbulkan bersifat dugaan kuat)	Hifdzul 'Irdh
7.	Pharming	Mengarahkan calon korban ke server web "kloning"	Pembentukan UU Perlindungan Data Pribadi	Mencuri data pribadi korban seperti nomor rekening bank, nama pengguna, kata sandi, nomor kartu kredit, dll	**Tipe Kedua** (sarana yang sejatinya tidak terlarang namun bisa menimbulkan potensi terjadinya tindakan yang dilarang)	**Tipe Kedua** (efek kerusakan yang akan ditimbulkan bersifat dugaan kuat)	Hifdzul 'Irdh

Bila tidak ada perlindungan Negara terhadap data pribadi, terkait dengan akses terhadap informasi, maka privasi warga negara dalam posisi yang rentan terhadap serangan siber yang dilakukan oleh pelaku *cyber crime*. Upaya perlindungan data pribadi ini juga menjadi tugas dan tanggungjawab Pemerintah guna mewujudkan kemaslahatan bagi warganya. Hal ini selaras dengan kaidah fikih:

تصرف الامام على الراعية منوط بالمصلحة

Artinya: "*Kebijakan pemegang kekuasaan (pemimpin) terhadap rakyat harus berdasarkan kemaslahatan*".

Nantinya, dalam pembuatan undang-undang tentang perlindungan data pribadi diharapkan mencakup prinsip, mekanisme dan sanksi, dapat juga mengadopsi beberapa aturan dalam GDPR (*General Data Protection Regulation*) seperti perjanjian pemilik data, pertanggungjawaban, penunjukan data pribadi. data manajemen, hak untuk menghapus dan mengakses data pribadi. Dengan demikian diharapkan dapat melindungi berbagai pihak dalam penyalahgunaan atau pencurian data pribadi dan memberikan sanksi bagi para pelaku kejahatan tersebut.

Sementara dalam perspektif fikih, pelaku tindakan pencurian data pribadi dapat dikenakan sanksi ta'zir karena mengingat mafsadatnya sekaligus melanggar privasi dan hak-hak dasar kemanusiaannya. Hingga akan berpotensi bahaya bila terjadi ketidakhadiran hukum pada perlindungan data pribadi akan sangat merugikan konsumen, karena ancaman dari pelanggaran selain kelalaian.

D. Kesimpulan

Munculnya era big data tidak hanya memberikan peluang penting bagi kemajuan sosial, tetapi juga membawa banyak ancaman keamanan informasi kepada masyarakat diantaranya tentang perlindungan terhadap privasi data pribadi. Dalam hukum Islam, data pribadi berisi kemuliaan, kehormatan, dan martabat seseorang yang tidak boleh diganggu. Ketika terjadi penyalahgunaan data, maka menimbulkan bahaya (mudharat) berupa rusaknya harkat dan martabat seseorang (hifz al-irdh) padahal syariat Islam sebisa mungkin mewujudkan kemaslahatan bagi manusia. Demi mewujudkan keamanan dan perlindungan privasi data, tidak hanya sejumlah besar teknologi keamanan informasi pribadi profesional yang dibutuhkan, tetapi juga hadirnya Negara yang

melindungi hak konstitusional serta menjamin privasi warganya agar tercipta ekosistem digital yang sehat. Untuk itu, sebagai aplikasi dari metode sadd dzari'ah, diaturnya perlindungan data pribadi dalam bentuk perundangan menjadi mutlak diperlukan sebagai langkah preventif guna menutup ruang kemafsadatan publik yang bisa ditimbulkan. Hal ini tidak lain sebagai upaya nyata Pemerintah dalam mewujudkan kemashlahatan dan menolak mafsadah bagi semua warga negaranya secara umum. Adanya perlindungan data privasi akan memperkuat sekaligus memperkokoh tingkat kepercayaan ekosistem digital.

E. Referensi

Agus, A. Aco, and Riskawati. "PENANGANAN KASUS CYBER CRIME DI KOTA MAKASSAR (Studi Pada Kantor Kepolisian Resort Kota Besar Makassar)." *Jurnal Supremasi* 11, no. 1 (2016): 20–29.

Al-Jauzi, Muhammad bin Abi Bakar Ayyub Azzar'i Abu Abdillah Ibnul Qayyim. *I'lamul Muwaqin*. Jilid 5., n.d.

Al-Zuhayliy, Wahbah. *Al-Wajiz Fi Usul Al-Fiqh*. Damaskus: Dar al-Fikr, 1999.

Ang, Millencia. "Consumer'S Data Protection and Standard Clause in Privacy Policy in E-Commerce: A Comparative Analysis on Indonesian and Singaporean Law." *the Lawpreneurship Journal* 1, no. 1 (2021): 100–113. http://journal.prasetiyamulya.ac.id/journal/index.php/TLJ/article/view/523.

Asyur, Muhammad Thahir Ibn. *Maqasid Syari'ah Al-Islamiyyah*. Petaling Jaya Malaysia: Dar An-Nafais, 2001.

Baroroh, Nurdhin. "Metamorfosis Illat Hukum Dalam Sad Adz-Dzari'ah Dan Fath Adz-Dzari'ah." *Al-Mazahib* 5, no. 2 (2017): 289–304.

Boccella, Nicola, Riccardo Misuraca, and Pierpaolo Tudisco Thor. "The Protection of Personal Data." *International Journal of Technology for Business (IJTB)* 2, no. 1 (n.d.): 43–54.

Burhani, Muhammad Hisyam Al. *Sadd Al Dzari'ah Fi Al-Syari'ah Al Islamiyyah*. Dar Kutub Ilmiyyah, n.d.

Bygrave, L. A. "Data Protection Pursuant to the Right to Privacy in Human Rights Treaties." *International Journal of Law and Information Technology* 6, no. 3 (1998): 247–284.

Dewi, Sinta. "Prinsip-Prinsip Perlindungan Data Pribadi Nasabah Kartu Kredit Menurut Ketentuan Nasional Dan Implementasinya." *Sosiohumaniora* 19, no. Vol 19, No 3 (2017): SOSIOHUMANIORA, NOPEMBER 2017 (2017): 206–212. http://jurnal.unpad.ac.id/sosiohumaniora/article/view/11380/6971.

Haganta, Raphael. "Legal Protection of Personal Data As Privacy Rights Of E-Commerce Consumers Amid The Covid-19 Pandemic." *Lex Scientia Law Review* 4, no. 2 (2020).

Hakim, Rahmat Nur. "Polri: Diduga Keras Data Kependudukan BPJS Kesehatan Bocor," n.d. https://nasional.kompas.com/read/2021/06/04/06300041/polri--diduga-keras-data-kependudukan-bpjs-kesehatan-bocor.

Hartono, Bambang. "Hacker Dalam Perspektif Hukum Indonesia," no. 26 (2011): 23–30.

Indonesia, CNN. "6 Bahaya Yang Intai Usai Kasus Data Bocor Tokopedia-Bukalapak." *2020*, n.d.

https://www.cnnindonesia.com/teknologi/20200506105640-185-500591/6-bahaya-yang-intai-usai-kasus-data-bocor-tokopedia-bukalapak.

Informasi, Kementerian Komunikasi dan. "Statistik Aduan." https://www.kominfo.go.id/statistik.

Intan arafah, Intan arafah. "Pendekatan Sadd Adz-Dzari'ah Dalam Studi Islam." *Al - Muamalat: Jurnal Hukum dan Ekonomi Syariah* 5, no. 1 (2020): 68–86.

Komarudin, Wahyudi Djafar dan Asep. *Perlindungan Hak Privasi Di Internet : Beberapa Kata Kunci*. Jakarta: Lembaga Studi dan Advokasi Masyarakat, 2014.

Pertiwi, Wahyunanda Kusuma. "Data Pengguna Tokopedia Bocor, Cek Apakah Akun Anda Terdampak," 2020. https://tekno.kompas.com/read/2020/05/03/11580057/data-pengguna-tokopedia-bocor-cek-apakah-akun-anda-terdampak.

———. "Facebook Didenda Rp 70 Triliun Akibat Skandal Cambridge Analytica," n.d. https://tekno.kompas.com/read/2019/07/14/08170087/facebook-didenda-rp-70-triliun-akibat-skandal-cambridge-analytica.

Pradana, Muh. Firmansyah. "Perlindungan Hukum Terhadap Pengguna Cloud Computing Atas Privasi Dan Data Pribadi." Tesis Program Studi Magister Kenotariatan Fakultas Hukum Universitas Hasanuddin Makassar, 2018.

Priscyllia, Fanny. "Perlindungan Privasi Data Pribadi Dalam Perspektif Perbandingan Hukum." *Jatiswara* 34, no. 3 (2019): 1–5.

Puluhulawa, Fenty Usman, Jufryanto Puluhulawa, and Moh. Gufran Katili. "Legal Weak Protection of Personal Data in the 4.0 Industrial Revolution Era." *Jambura Law Review* 2, no. 2 (2020): 182–200.

Rahmawati, Ineu. "The Analysis Ofcyber Crime Threat Risk Management To Increase Cyber Defense." *Jurnal Pertahanan & Bela Negara* 7, no. 2 (2017): 51–66.

Rosadi, Sinta. "Protecting Privacy On Personal Data In Digital Economic Era : Legal Framework In Indonesia." *Brawijaya Law Journal* 5, no. 2 (2018): 143–157.

Sa'diyah, Nur Khalimatus. "Modus Operandi Tindak Pidana Cracker Menurut Undang-Undang Informasi Dan Transaksi Elektronik." *Perspektif* 17, no. 2 (2012): 78.

Salleh, Ahmad Dahlan, Mohd Izhar Ariff Mohd Kashim, Nurul Ilyana Muhd Adnan, Nik Abdul Rahim Nik Abdul Ghani, and Ezad Azraai Jamsari. "Theory and Application of Sadd Al-Dhara'i' (Blocking the Means) in Shafi'iyya School." *International Journal of Academic Research in Business and Social Sciences* 9, no. 1 (2019): 724–737.

Setiawati, Diana, Hary Abdul Hakim, and Fahmi Adam Hasby Yoga. "Optimizing Personal Data Protection in Indonesia: Lesson Learned from China, South Korea, and Singapore." *Indonesian Comparative Law Review* 2, no. 2 (2020): 2–9.

Sitompul, Asri. *Hukum Internet, Pengenalan Mengenai Masalah Hukum Di Cyberspace*. Bandung: Citra Aditya Bakti, 2001.

Soediro, Soediro. "Prinsip Keamanan, Privasi, Dan Etika Dalam Undang-Undang Informasi Dan Transaksi Elektronik Dalam Perspektif Hukum Islam." *Kosmik Hukum* 18, no. 2 (2018): 95–112.

Suhariyanto, B. *Tindak Pidana Teknologi Informasi (Cyber Crime) Urgensi Pengaturan Dan Celah Hukumnya*. Jakarta: Rajawali Press, 2014.

Sujadmiko, Bayu. "The Urgency of Digital Right Management on Personal Data Protection." *INTERNATIONAL JOURNAL OF RESEARCH IN BUSINESS AND SOCIAL SCIENCE* 10, no. 1 (2021): 253–258.

Syatibi, Al. *Al Muwafaqat*. Juz III. Mesir: Matba'ah al Maktabah al Tijariyah, n.d.

Zuhaily, Wahbah al. *Ushul Fiqh Al Islamy*. Juz II. Dar al-Fikr, 1986.