

LAPORAN PRAKTIKUM

Sesi# 7

E-BISNIS

Disusun oleh

Vina Sahara

NPM 23753038

Sebagai salah satu syarat untuk tugas e-bisnis

Manajemen informatika

Jurusan teknologi informasi



POLITEKNIK NEGERI LAMPUNG

BANDAR LAMPUNG

2025

KEBIJAKAN PUBLIK PADA E-BISNIS

Kebijakan publik adalah serangkaian tindakan, keputusan, strategi, atau peraturan yang dibuat oleh pemerintah. Tindakan yang diambil bisa melalui hukum UUD, kebijakan publik juga tidak hanya berupa undang-undang, tetapi juga meliputi program, peraturan teknis, dan kegiatan pemerintah yang mempengaruhi kehidupan masyarakat luas. Bertujuan untuk mengatasi masalah publik serta mencapai tujuan.

Ruang lingkup kebijakan publik tidak lagi terbatas pada sektor konvensional, tetapi juga meluas ke bidang ekonomi digital. Salah satu wujudnya adalah munculnya kebijakan publik dalam e-bisnis, yaitu kebijakan pemerintah yang mengatur dan mengarahkan kegiatan bisnis berbasis elektronik agar berjalan aman, adil, dan sesuai dengan peraturan yang berlaku.

Kebijakan publik pada e-bisnis adalah seperangkat aturan hukum dan regulasi yang dibuat pemerintah untuk mengatur dan mengembangkan kegiatan e-bisnis, memastikan transaksi yang aman, adil, dan terpercaya bagi semua pihak. Fokus utama kebijakan ini meliputi penegakan hukum, perlindungan konsumen, pajak e-commerce, perlindungan data pribadi, dan dukungan untuk UMKM dan inovasi digital.

1. Penyelenggara Sistem Elektronik Lingkup Privat

Peraturan ini mengatur tentang kewajiban dan tanggung jawab penyelenggara sistem elektronik (PSE) lingkup privat, yaitu perusahaan digital seperti marketplace, media sosial, aplikasi pesan, dan penyedia layanan online lainnya.

Permenkominfo No. 5 Tahun 2020 mewajibkan setiap platform digital yang beroperasi di Indonesia mendaftar ke Kementerian Kominfo, menghapus konten yang melanggar hukum, dan melindungi data pengguna.

Selain itu, peraturan ini menjadi dasar bagi pengawasan aktivitas digital seperti penyebaran hoaks, penipuan online, hingga transaksi ilegal di dunia maya.

a) Tujuan

- Menjamin keamanan dan ketertiban ruang digital nasional.
- Melindungi masyarakat dari konten berbahaya dan aktivitas e-bisnis ilegal.
- Menegaskan tanggung jawab platform digital terhadap data dan perilaku pengguna.

b) Proses

- Pemerintah Pusat (Kominfo): membuat regulasi, membuka pendaftaran PSE, dan mengawasi penerapan aturan
- Daerah (Dinas Kominfo): melakukan sosialisasi, pendataan, dan menindaklanjuti laporan masyarakat terkait pelanggaran digital.
- Pelaku E-Bisnis (Platform Digital): mendaftar resmi ke Kominfo, menerapkan sistem moderasi konten, dan menindak akun bermasalah.
- Individu (Masyarakat/Pengguna): mematuhi aturan penggunaan platform dan melapor jika menemukan pelanggaran.

c) Dampak

- Ruang digital menjadi lebih tertib dan aman.
- Meningkatnya kepercayaan pengguna terhadap platform lokal dan asing.
- Penurunan jumlah konten negatif, penipuan online, dan aktivitas ilegal.

d) Alur Penurunan Kebijakan

- 1) Kominfo (Kementerian Komunikasi Dan Informatika Republic Indonesia)

Proses yang Dilakukan:

- Menyusun dan menetapkan regulasi nasional
- Membentuk sistem dan standar nasional

- Melakukan pengawasan dan evaluasi nasional
- Menyediakan sistem pelaporan dan aduan publik nasional

2) Diskominfo Daerah (Dinas Kominfo di tingkat Provinsi atau Kabupaten/Kota)

Proses yang Dilakukan:

- Sosialisasi kebijakan pusat ke daerah
- Pendampingan teknis dan edukasi e-bisnis
- Koordinasi dan pelaporan ke Kominfo pusat
- Kolaborasi dengan instansi daerah lain

3) Platform Digital (Perusahaan E-Bisnis / PSE)

Proses yang dilakukan:

- Registrasi dan legalisasi ke Kominfo
- Penerapan sistem keamanan dan moderasi
- Kepatuhan dan pelaporan berkala ke Kominfo
- Kolaborasi dengan aparat dan Diskominfo daerah

4) Pengguna Individu (Masyarakat / Konsumen Digital)

Proses yang dilakukan:

- Mengikuti kebijakan dan aturan digital nasional
- Meningkatkan literasi digital
- Menggunakan kanal pelaporan resmi
- Berpartisipasi aktif dalam ekosistem e-bisnis

2. Penyelenggaraan Sistem dan Transaksi Elektronik

Kebijakan ini menetapkan standar nasional dalam penyelenggaraan sistem elektronik dan keamanan transaksi digital yang wajib diterapkan oleh seluruh pelaku bisnis berbasis elektronik, baik instansi pemerintah.

Peraturan ini mencakup ketentuan mengenai pengelolaan dan perlindungan data pribadi, penerapan sistem keamanan jaringan yang andal,

jaminan keutuhan serta ketersediaan layanan elektronik, dan perlindungan hukum bagi pengguna dalam setiap aktivitas transaksi online.

a) Tujuan

- Menjamin keamanan dan keandalan sistem transaksi elektronik.
- Menjaga kerahasiaan dan integritas data digital pengguna.
- Meningkatkan kepercayaan masyarakat terhadap layanan e-bisnis nasional.

b) Proses

- Pusat (Kominfo dan BSSN): menetapkan standar keamanan data (misalnya enkripsi, sertifikat elektronik, audit sistem).
- Daerah (Diskominfo): memantau dan membantu pelaku usaha lokal dalam menerapkan sistem keamanan digital.
- Pelaku E-Bisnis: menerapkan teknologi keamanan seperti SSL, OTP, firewall, dan autentikasi pengguna.
- Individu: menjaga keamanan akun, menggunakan layanan resmi, dan tidak membagikan data pribadi sembarangan.

c) Dampak

- Transaksi digital menjadi lebih aman dari peretasan atau penyalahgunaan data.
- Menurunnya kasus pencurian identitas digital.
- Terbangunnya ekosistem bisnis online yang terpercaya.

d) Alur Penurunan Kebijakan

Tingkat	Pelaksana	Peran dan Proses yang Dilakukan	Tujuan Utama
---------	-----------	---------------------------------	--------------

Tingkat Pusat	Kominfo & BSSN (Badan Siber dan Sandi Negara)	<p>a. Perumusan Kebijakan Nasional – Menetapkan pedoman keamanan siber, tata kelola data pribadi, dan standar teknis sistem elektronik.</p> <p>b. Sertifikasi dan Pengawasan Sistem Elektronik – BSSN melakukan sertifikasi keamanan sistem bagi penyelenggara e-bisnis (misalnya marketplace, bank digital, fintech).</p> <p>c. Penegakan Kepatuhan dan Audit Keamanan – Kominfo melakukan audit terhadap perusahaan digital yang menyimpan data masyarakat.</p> <p>d. Koordinasi Nasional – Kominfo dan BSSN bekerja sama dengan lembaga lain (OJK, BI, Kemenkumham) untuk memastikan perlindungan data lintas sektor.</p> <p>e. Pembuatan Sistem Nasional Keamanan Data seperti <i>Cyber Security Incident Response Center (CSIRT)</i> dan <i>Indonesia Security Operations Center (ISOC)</i>.</p>	Menetapkan standar nasional dan menjamin keamanan serta legalitas sistem elektronik di Indonesia.
---------------	--	--	---

Tingkat Daerah	Diskominfo Daerah (Provinsi/Kota/Kabupaten)	<p>a. Implementasi dan Sosialisasi Kebijakan – Menyebarluaskan peraturan PSTE ke pelaku usaha dan masyarakat daerah.</p> <p>b. Pembinaan dan Pendampingan UMKM Digital – Membantu pelaku bisnis kecil menengah dalam menerapkan keamanan siber (misalnya penggunaan SSL, enkripsi data, atau backup server).</p> <p>c. Koordinasi dengan BSSN/Kominfo Pusat – Melaporkan insiden kebocoran data atau gangguan sistem di wilayahnya.</p> <p>d. Edukasi Literasi Digital – Melatih masyarakat agar memahami cara aman bertransaksi online dan melindungi data pribadi.</p>	<p>Menerjemahkan kebijakan pusat agar dapat dijalankan di tingkat lokal dan melindungi pelaku usaha serta masyarakat di daerah.</p>
----------------	--	--	---

Tingkat Pelaku Usaha	Pelaku E-Bisnis (Marketplace, Fintech, Bank Digital, Startup, UMKM Online)	<p>a. Kepatuhan terhadap Regulasi PSTE – Mendaftarkan sistem elektronik ke Kominfo dan memastikan legalitas penyelenggara. b. Keamanan Sistem dan Data – Menerapkan enkripsi, firewall, autentikasi ganda, serta melakukan backup data secara rutin. c. Perlindungan Pengguna – Menyediakan kebijakan privasi, layanan pengaduan, dan transparansi dalam penggunaan data pelanggan. d. Audit Internal dan Pelaporan Berkala – Melaporkan kepada Kominfo bila terjadi insiden atau pelanggaran data. e. Edukasi Konsumen – Mengajak pengguna untuk menjaga keamanan akun dan tidak membagikan OTP/kata sandi.</p>	Menjamin keamanan transaksi, membangun kepercayaan pelanggan, dan mencegah kebocoran data pribadi.
-----------------------------	---	---	--

Tingkat Individu	Masyarakat (Pengguna Layanan E-Bisnis)	<p>a. Partisipasi dan Kepatuhan Digital – Menggunakan sistem elektronik resmi yang sudah terdaftar di Kominfo. b. Kesadaran Keamanan Pribadi – Menjaga kerahasiaan data (seperti NIK, PIN, OTP, dan password). c. Pelaporan Insiden Digital – Melapor ke platform atau pihak berwenang bila mengalami penipuan, kebocoran data, atau aktivitas mencurigakan. d. Edukasi Mandiri – Mengikuti pelatihan literasi digital dan memahami hak-hak perlindungan data pribadi.</p>	Meningkatkan kesadaran masyarakat terhadap keamanan data dan membangun budaya digital yang aman dan bertanggung jawab.
------------------	---	--	--

3. Permenkominfo Peraturan Anti Penipuan & Pengawasan Platform Digital

Kebijakan ini merupakan bagian dari regulasi pengawasan dan penindakan terhadap konten negatif, akun penipuan, dan aktivitas ilegal di platform digital. Diatur dalam beberapa pasal turunan Permenkominfo No. 5 Tahun 2020 dan diperkuat dengan kebijakan Kominfo serta Kepolisian Republik Indonesia.

Kebijakan ini mewajibkan platform digital seperti Tokopedia, Shopee, Meta, atau X (Twitter) untuk menghapus akun penipu, menindak

pelaku penipuan online, serta menyediakan sistem pelaporan yang mudah diakses masyarakat.

a) Tujuan

- Mencegah dan menindak penipuan online di e-commerce dan media sosial.
- Melindungi hak-hak konsumen dalam transaksi digital.
- Menciptakan lingkungan e-bisnis yang aman dan transparan.

b) Proses

- Pusat (Kominfo & Kepolisian): menetapkan mekanisme pelaporan dan penghapusan konten penipuan digital.
- Daerah (Diskominfo & Kepolisian Daerah): menerima laporan masyarakat dan menindak akun pelaku penipuan.
- Platform E-Bisnis: memverifikasi identitas penjual dan menonaktifkan akun mencurigakan.
- Individu: berhati-hati dalam transaksi dan melapor jika terjadi penipuan.

c) Dampak

- Kasus penipuan online menurun.
- Kepercayaan masyarakat terhadap transaksi digital meningkat.
- Pelaku e-bisnis menjadi lebih bertanggung jawab terhadap keamanan konsumen.

d) Alur Penurunan Kebijakan

1) Penyusunan & Penetapan Regulasi Nasional

- Kominfo menetapkan pedoman resmi penanganan konten penipuan, penyebaran hoaks, atau aktivitas ilegal digital.
- Bekerja sama dengan Polri (Direktorat Siber Bareskrim) untuk menyusun standar penegakan hukum siber.

2) Membangun Sistem Pelaporan Terpadu Nasional

- Melalui aduankonten.id (untuk laporan publik) dan patroli siber (patrolisiber.id) untuk memantau konten atau akun penipuan.

- Kominfo dan Polri menindak akun/website yang terindikasi penipuan dengan pemblokiran, takedown, atau proses hukum.

3) Koordinasi Antarlembaga dan Platform

- Kominfo mengeluarkan surat edaran dan teguran resmi kepada platform digital (seperti Shopee, Meta, Tokopedia) untuk menonaktifkan akun penipu.
- Polri menangani investigasi hukum bila penipuan digital mengandung unsur pidana.

4) Publikasi dan Edukasi Nasional

- Melalui kampanye “Lindungi Data Pribadimu” dan “Cerdas Digital Tanpa Tipu-Tipu Online”.
- Tujuannya meningkatkan literasi masyarakat terhadap modus penipuan online.